USING ARTIFICAL INTELLIGENCE TOOLS FOR RISK ASSESSMENT IN THE PROJECT MANAGEMENT FOR IT INDUSTRY

by

<PURANDHAR TUMKUR PHANINDRA>

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

<JUNE, 2023>

USING ARTIFICAL INTELLIGENCE TOOLS FOR RISK ASSESSMENT IN THE PROJECT MANAGEMENT FOR IT INDUSTRY

by

<PURANDHAR TUMKUR PHANINDRA>

APPROVED BY

____
Dr. Saša Petar, Ph.D., Chair

Anna Provodnikova
Dr. Anna Provodnikova, Ph.D., Committee Member

____
Dr. Ljiljana Kukec, Ph.D., Committee Member

RECEIVED/APPROVED BY:

____
SSBM Representative

Dedication

I would like to dedicate this thesis to my parents Phanindra T K and Parimala T P. Thank you so much for everything! Words can hardly describe my thanks and appreciation to you. You have been my source of inspiration, support, and guidance. You have taught me to be unique, determined, to believe in myself, and to always persevere. I am truly thankful and honored to have you as my parents. To take a quote from Albert Schweitzer, “At times our own light goes out and is rekindled by a spark from another person. Each of us has cause to think with deep gratitude of those who have lighted the flame within us”. You, mom, and dad, have been that spark for me when my light blew out. Thank you for your unwavering love and support along this journey I have taken. I love you both always and forever.

Acknowledgements

Words cannot express my gratitude to my guide Dr. Ljiljana Kukec for her invaluable patience and feedback. I also could not have undertaken this journey without her support who generously provided knowledge and expertise. Additionally, this endeavor would not have been possible without the generous support of my spouse Poojitha N.

.

ABSTRACT

USING ARTIFICAL INTELLIGENCE TOOLS FOR RISK ASSESSMENT IN THE PROJECT MANAGEMENT FOR IT INDUSTRY

<PURANDHAR TUMKUR PHANINDRA >
<2023>

Dissertation Chair: <Chair's Name>
Co-Chair: <If applicable. Co-Chair's Name>

Risk is an integral part of any project and it's more appropriate to say for IT Industry because it is changing with a very fast pace. Different surveys, reports and research show astonishing statistics about the risks in projects of IT Industry. Through proper risk assessment techniques most of the uncertainties can be reduced while initiating, implementing, and improving IT projects. Different authors talk about different risks and different strategies to respond to them. It becomes difficult at times to keep in check all the risks. Often risk management is over hyped, and often it's totally neglected. Their needs to be a balanced approached in risk management. The aim of this research project is to develop and analyze a structured approach using Artificial Intelligence which will help organization in identifying & categorizing risks and measuring their impact on projects in IT Industry well in advance.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I:

INTRODUCTION

1.1 Introduction

Risks are an inevitable part of life. A risk is any possible outcome or event that can occur over the course of a project or during a process. Risks can be related to timeline, budget, or performance, but there is no limit to its flavors. Project risk management is the process of making educated guesses and mapping out strategies related to these perceived risks. (Gertz, 2022).

Understanding risks allows us to plan more accurately, learn from our mistakes, and create smoother processes for future projects. It also helps to estimate time, money, and people resources better, which is good news for project team, company & clients. (Gertz, 2022).

It can be tempting to skimp on this stage and push these little risks under the rug or to ignore them altogether. But ignoring them does not make them disappear. They will come back and bite, and when we are not prepared, they can kill an entire project. Nothing is more important to the success of a project than a project manager’s ability to identify and manage risk. (Gertz, 2022).

While it is easy to assume all risk is bad, these impacts could have either a positive or negative effect on the project. It is less about the outcome and more about the uncertainty of factors that could cause your plan to shift, for better or worse. (LaPrad, 2020).

The proper risk management can bring the projects closer to success. It is important to consider all pros and cons before delivering the work. The result may vary depending on the right analysis of the risk. If we do not follow the right methods, we will end up with either unsuccessfully finished project and not giving it the full potential, or with a complete failure and the project's loss. It is worth to spend a while on predicting & analyzing risk to create the best outcomes. (Ray, 2021).

Different authors talk about different risks and different strategies to respond to them. It becomes difficult at times to keep in check all the risks and all strategies. Often risk management is over hyped, and often it is totally neglected. There needs to be a balanced approached in risk management.

The outcome of this research will bring significant contribution to project risk management as a key discipline of project management and enhance project success for IT industry.

1.2 Research Problem

Project management is a complex process that involves planning, organizing, and controlling resources to achieve specific goals within a set timeframe. In the IT industry, project management is critical as it helps to ensure that projects are delivered on time, within budget, and to the required quality standards. One of the key challenges in project management is identifying and managing risks that can impact project success.

Risk assessment is a critical component of project management, as it helps project managers to identify potential risks and develop strategies to mitigate or manage them.

The IT industry is constantly evolving, and project managers are often faced with new and complex challenges when managing IT projects. One of the critical challenges in project management for the IT industry is identifying and managing risks that can impact project success.

Traditional methods of risk assessment may not be sufficient in the rapidly changing and complex IT environment. Therefore, there is a need to explore the use of Artificial Intelligence tools for risk assessment in project management for the IT industry.

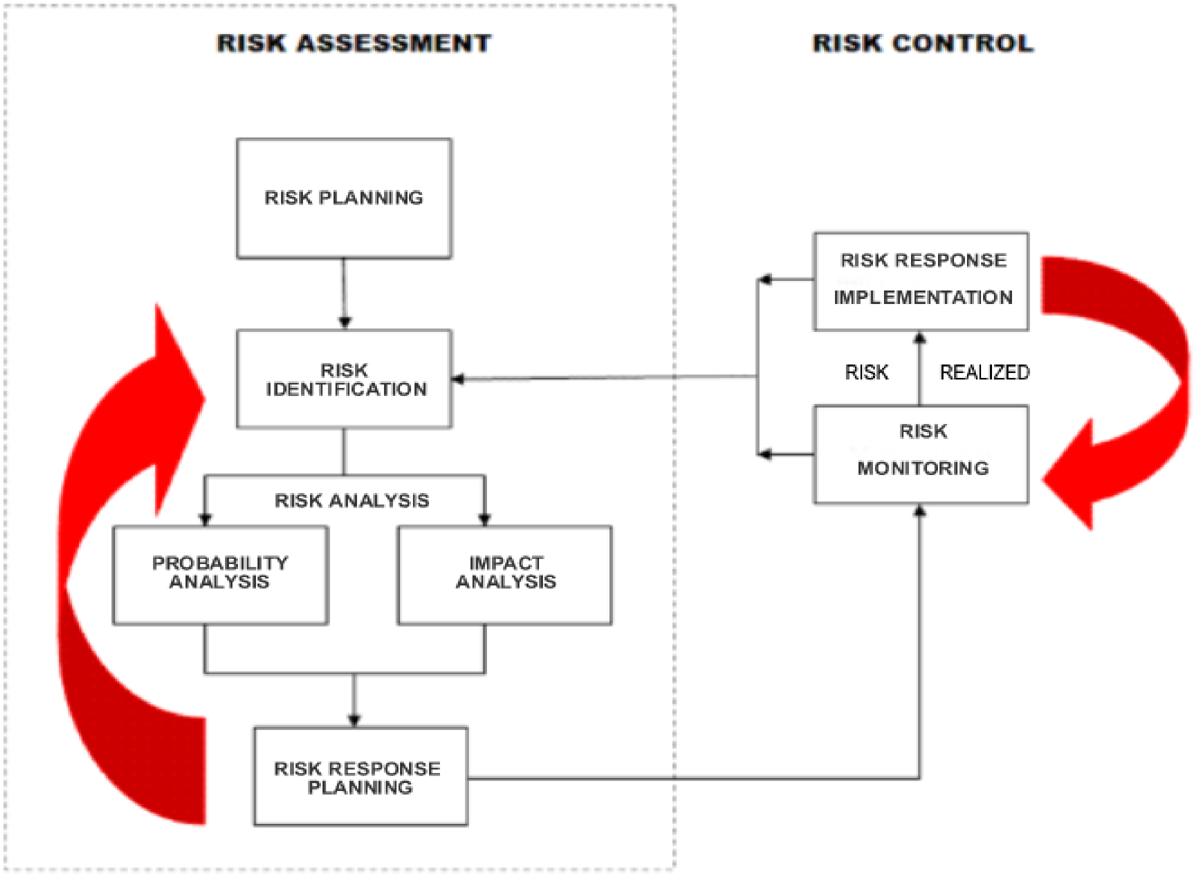


Figure 1: Risk Assessment Framework.

(Source: Frohnhoefer, R.W. (2019), Risk Assessment Framework.)

1.3 Purpose of Research

The purpose of this study is to provide a better understanding of risks related to Projects of IT Industry. This study will elaborate on how to identify risks and their impact on IT Projects. It will also provide with an understanding about what different schools of thought say about Risks in project management of IT Industry.

Artificial Intelligence can be used for risk assessment in project management to identify and manage potential risks that may arise during a project's lifecycle. This can help project managers take proactive measures to mitigate risks and ensure the project's success.

The research question of this dissertation is to develop and analyze a structured approach which will permit an organization in identifying & categorizing risks and measuring their impact on IT Projects.

Particularly, the study has the following sub-objectives:

a) **Improved Risk Assessment:** Artificial Intelligence tools can help project managers to identify potential risks more accurately and quickly than traditional methods.

b) **Early Warning Systems**: Artificial Intelligence tools can be used to develop early warning systems that can alert project managers to potential risks before they become critical.

c) **Improved Decision Making**: Artificial Intelligence tools can provide project managers with data-driven insights that can help them to make informed decisions about risk management.

d) **Increased Efficiency**: Artificial Intelligence tools can automate many of the manual processes involved in risk assessment, which can save time and Resources.

e) **Innovation and competitiveness**: The use of Artificial Intelligence tools for risk assessment in project management can help organizations to stay competitive and innovative. By leveraging the power of Artificial Intelligence, organizations can gain a competitive advantage by identifying and managing risks more effectively and efficiently than their competitors.

1.4 Significance of the Study

The significance of this research is that it has the potential to revolutionize project management in the IT industry. Using artificial intelligence (AI) tools for risk assessment, this research paper addresses the limitations of traditional approaches and explores the benefits and challenges of using Artificial Intelligence in risk management.

a) **Advances in Risk Assessment**: This research contributes to the advancement of risk assessment in project management. Leadership often relies on guidelines and concepts that may miss critical or immutable aspects of a changing project. By using artificial intelligence tools, the project manager can develop risk identification, analysis, and mitigation strategies to provide more efficient and effective risk management.

b) **Improving project outcomes**: This research paper shows how Artificial intelligence can impact outcome in the IT industry. Using Artificial intelligence capabilities such as data analysis, pattern recognition and real-time monitoring, project managers can make informed decisions, identify opportunities early on, and take action to mitigate them. In turn, this increases project efficiency, reduces costs, shortens timelines, and improves progress.

c) **Enhanced decision support**: Artificial intelligence tools provide effective decision support to project managers. Artificial intelligence algorithms can analyze large amounts of project-related data to generate recommendations and recommendations for risk reduction strategies. This enables project managers to make data-driven decisions, allocate resources effectively, and prioritize risk responses to achieve better results.

d) **Adoption of technology development**: A study supporting the use of new technologies in project management in the IT sector. Artificial intelligence tools represent a technology that could revolutionize the practice of risk assessment. By using Artificial intelligence, organizations demonstrate their passion for using new technologies to improve project outcomes, quickly making them more competitive in a changing IT environment.

e) **Practical implications**: This research paper provides useful implications for project managers and IT professionals who want to incorporate Artificial intelligence into their risk assessment. It explores the benefits of using Artificial intelligence, identifies potential challenges, and provides insight into the integration process, the need for Artificial intelligence, and transforming decision-making. This can serve as valuable advice for organizations looking to implement Artificial intelligence E-driven strategic risk assessment.

f) **Contribution to knowledge**: This study adds to the knowledge of the application of project management skills, particularly in the context of risk management research in the IT industry. By combining previous research and presenting new evidence, this research paper expands the understanding of the effective use of Artificial intelligence tools for risk assessment, thereby enriching the literature article on Artificial intelligence and project management.

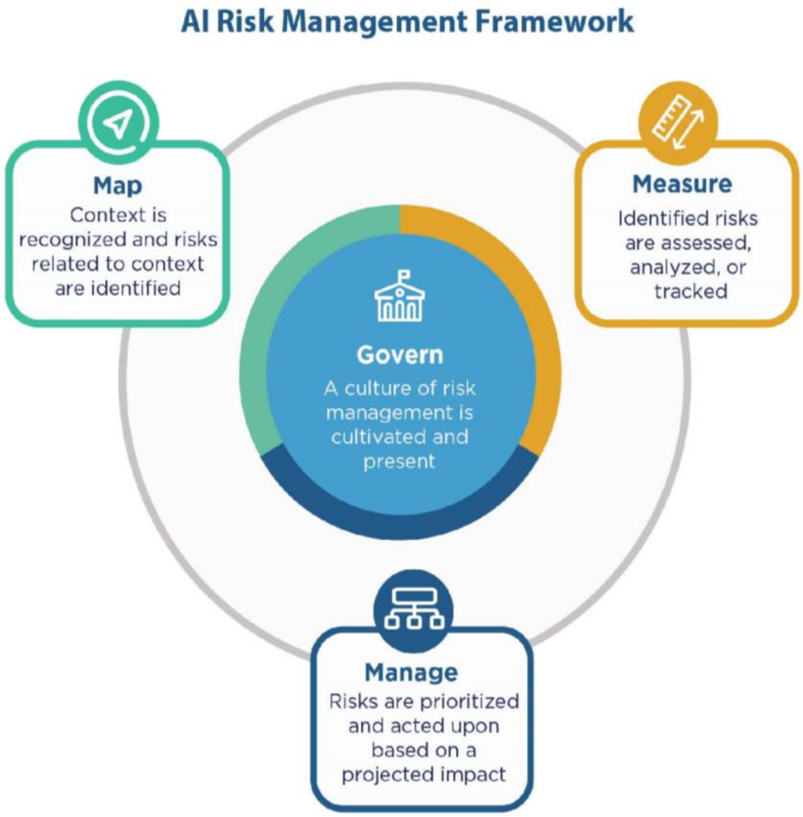

AI Risk Management Framework
Map
Context is recognized and risks related to context are identified
Measure
Identified risks are assessed, analyzed, or tracked
Govern
A culture of risk management is cultivated and present
Manage
Risks are prioritized and acted upon based on a projected impact

Figure 2: Artificial Intelligence Risk Management Framework

(Source: Department of Defense (2019), DoD Digital Modernization Strategy.)

In conclusion, the importance of this research paper lies in its ability to drive innovation, improve project outcomes, and strengthen risk assessment in business IT. By highlighting the benefits, challenges, and implications of using Artificial intelligence tools for risk assessment in project management, the research provides insights to practitioners and contributes to a broader understanding of the role Artificial intelligence plays in the field.

1.5 Research Purpose and Questions

The purpose of this study is to examine the importance of using artificial intelligence (AI) tools for risk assessment in project management in the IT industry. This study aims to explore the benefits and challenges of integrating Artificial intelligence into the risk assessment process and its impact on outcomes. Addressing the limitations of traditional approaches and exploring the potential of expertise, this research focuses on the application of risk assessment and contributes to the improvement of management in the IT industry.

Research questions:

a) What are the limitations of risk assessment in project management in the IT industry?

b) How to Use Artificial Intelligence Tools to Improve Risk Assessment in Project Management in the IT Industry?

c) What are the benefits of using Artificial intelligence tools for risk assessment in the IT industry?

d) What are the challenges and limitations of integrating Artificial intelligence into risk assessment processes?

e) How does the integration of Artificial intelligence tools for risk assessment affect outcome in the IT industry?

f) What are the critical success factors for using Artificial intelligence tools to assess risk in the IT industry?

g) What are the implications of using Artificial intelligence tools for risk assessment in project management in the IT industry?

This research question provides a basis for exploring the importance of using Artificial intelligence tools for risk assessment in project management in the IT industry. They aim to assess the limitations of traditional methods, examine the benefits and challenges of Artificial intelligence integration, evaluate the impact of the event, and determine the importance of implementation and its impact on project management.

CHAPTER II:

REVIEW OF LITERATURE

2.1 Theoretical Framework

The theoretical framework of this research paper can be built on two main themes: Artificial Intelligence (AI) in risk management and project management.

Project Risk Management: The Project Risk Management Framework provides a framework for understanding traditional methods for risk assessment in management in the IT industry. It includes theories, models, and best practices for identifying and mitigating risks in the project environment. Theories and concepts may include the Management Information Group, risk management systems and information on standard risk assessment.

Artificial Intelligence in Project Management: The Artificial Intelligence Framework focuses on theories, models, and strategies for using Artificial Intelligence tools to take risks in project management. The framework can draw insights and ideas from artificial intelligence, machine learning, natural language processing, and data analysis. Key topics of interest include Artificial Intelligence algorithms, data mining, pattern recognition, modeling, and decision support.

The combination of these two points lays the foundation for understanding the importance of using Artificial Intelligence tools for risk assessment in project management in the IT industry. It allows to examine the limitations of traditional risk assessments as well as the benefits that Artificial Intelligence tools can provide. This theoretical framework provides a lens through which the impact of Artificial Intelligence integration on project outcomes, stakeholder engagement and decision-making can be analyzed.

This research paper provides a better understanding of the importance of using artificial intelligence tools for risk assessment in business management by integrating the theoretical framework. It explores the theoretical basis, practical implications, and future potential of the field, ultimately contributing to knowledge and guiding managers and organizations in applying artificial intelligence to risk management.

2.2 Theory of Reasoned Action

The increasing working efficiency of different components is reducing the time, speed, size, and complexity of computer systems which have been facilitating a shift from batch to real time processing. A change can also be seen in technology at enterprise and global level from mainframe era to client server and then shared, networked IT infrastructure. It has always been difficult to make quick and right decisions in continuously changing environment. Niccolò Machiavelli et al (1955) wrote in The Prince, "There is nothing more difficult to plan, more doubtful of success, nor more dangerous to manage than the creation of new system". In today's competitive environment organizations are more IT dependent than ever before. Short span of time to complete a project is increasing pressure on management to make hasty decisions without proper consideration of risks which delimits the project success even by spending more time and resources (Hinde, 2005).

Risk is an integral part of any project, and it is more appropriate to say for IT because it is changing with an extremely fast pace. Different surveys, reports and research show astonishing statistics about the risks of projects in IT industry.

According to The Standish Group International (2001), different surveys and reports indicate that 23% of projects are canceled while 49% went beyond their cost estimation. (Tiwana et al, 2007). Moreover, in another report Standish group reveals that U.S spent $275 billion on software development every year and above 70 % of those projects do not get success because of inflated cost or schedule overrun whereas some of them fulfill certain specification or fails entirely. (Wallace et al, 2004). Research by McFarlan et al (2003) reveals that from 1997 to 2001, $2.5 trillion spent on IT projects but $1 trillion were unsafe because of bad execution and most of them eventually collapsed. (Keil et al, 2004). In March 2004 UK national Audit Office analyzed 250 IT projects of the last two years. Half were incomplete and more than quarter were at elevated risk. (Hinde, 2005). Furthermore, In 1997 KPMG International consulting firm hold a survey and reported that 60% of the failed projects had the expectation to be finished within a year. (Whittaker, 1999). Furthermore, in US 80% of IT projects are funded which do not have any proper planning (McFarlan et al, 2003).

Through proper risk assessment techniques most of the uncertainties can be reduced while initiating, implementing, and improving projects. The OTR Group (1992) discovered that organizations are spending only 30 % for risk assessment associated with IT spending and project management. (Baccarini et al, 2004). There is a wide range of risks and possibilities to eliminate those risks while managing projects. It is also worthwhile to be aware of those risks while making strategies and taking decision for a new project plan and proposal.

Different authors talk about different risks and different strategies to respond to them. It becomes difficult at times to keep in check all the risks and all strategies. Often risk management is over hyped, and often it is totally neglected. There needs to be a balanced approached in risk management.

2.3 Theory

Project failure is an ongoing issue in IT industry projects. During the relative infancy of computerized information systems in the 1960s, the difficulties of software project management and associated project failure were traced to inadequate system definition, improper vesting of responsibility, inherent complexity, and fascination with technology to the detriment of meeting business needs (Reel 1999). Recent authors have concluded that software projects fail due to the inconsistent use of estimation metrics, complexity in both the design and implementation of software, insufficient experiences staff available to complete project tasks, inadequate project management (Reel 1999).

Another explanation for the high failure rates in software projects is "that managers are not taking prudent measures to assess and manage the risks involved in these projects". But taking prudent risk management measures may be hindered by the complexity encountered when attempting to collect sufficient information to develop an informed judgment. It is rarely sufficient to simply ask other project participants for their views about a project's status and its associated risks. Understanding a project's risk characteristics requires reliable information. (Reel 1999).

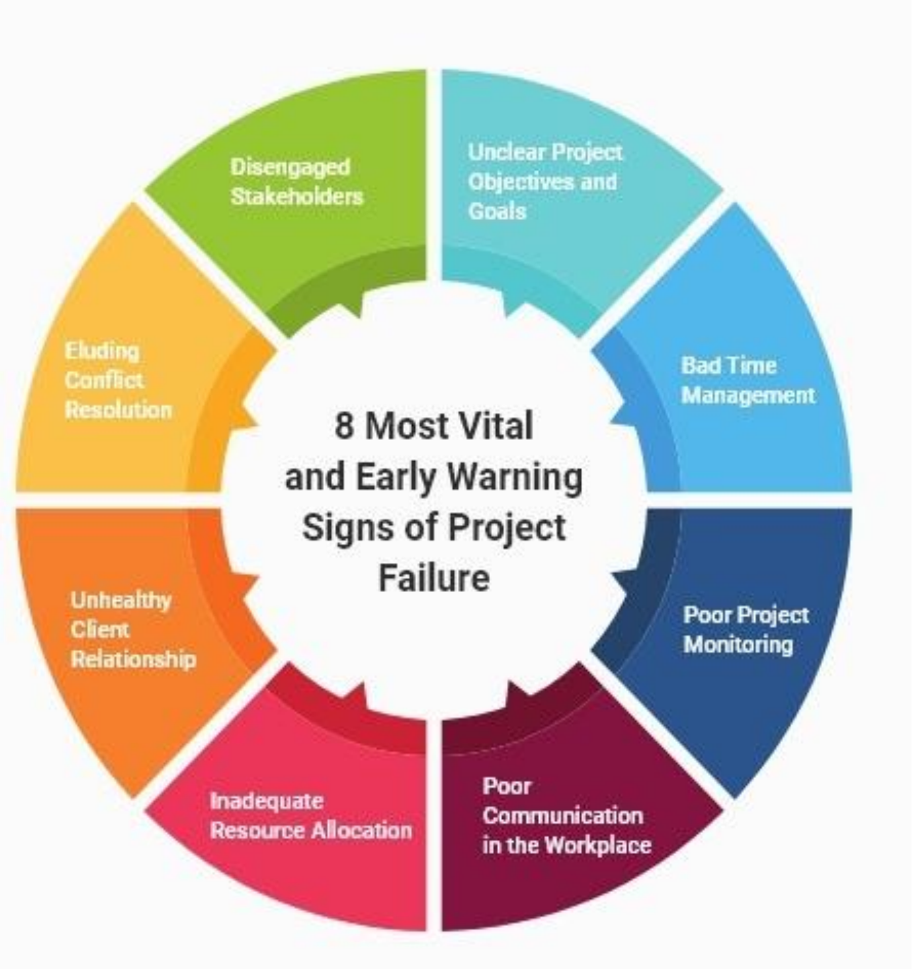

8 Most Vital and Early Warning Signs of Project Failure
Disengaged Stakeholders
Unclear Project Objectives and Goals
Bad Time Management
Poor Project Monitoring
Poor Communication in the Workplace
Inadequate Resource Allocation
Unhealthy Client Relationship
Eluding Conflict Resolution

Figure 3: Early Warning signs of Project Failure

(Source: ProProfs Project Blog. (2017), Why Do Projects Fail?)

2.3.1 What is risk?

There are lots of definitions of risks but there is no comprehensive definition which can be used universally. Most of them have these two basic characteristics.

"**Uncertainty**: An event may or may not happen.

Loss: An event has unwanted consequences or losses" (Neill et al, 2001).

A formal definition of risk is "*The probability that the actual input variables and the outcome results may vary from those originally estimated, the variation between the actual and the ending result shows the level of the risk*" (Remenyi, 1999).

Risk is defined in a very simple way "*A problem that hasn't happened yet but could cause some loss or threaten the success of your project if it did*" (Wiegers, 1998.).

Apart from benefits IT has brought lots of risks which need to be properly identified and a project manager should keep in mind all those risks before going to start a new project or to rectify existing risks in ongoing projects.

Characteristics of risks described by Taylor (2004), were divided in three parts:

a) The event (i.e., any negative or positive incident taking place to the project)

b) The probability of event occurrence (i.e., what is the possibility of happening that event)

c) The impact to the project (when at last the event takes place what would be its consequences, negative or positive)

One of the key factors for risk management success is documenting and using the lessons learned from each project. Without a documented chronicle of what went right, what went wrong, the reasons for both, and the solutions to problems, an organization cannot improve its project success rate. Managing risks is the key to project success.

2.3.2 Predictable and Unpredictable Risks

All risks do not influence the project negatively. Risk may have an opportunity which can help to get hold of positive outcome. Taylor (2004) divides the risks into two main types:

a) Business Risks
b) Insurable or Pure Risks

Business risks might impact the project in both, positive and negative way but these risks are considered as manageable risks. For example, if an organization required more resources to fulfill the project needs, the required resources can be acquired by hiring etc.

On the other hand, insurable or pure risks are difficult to manage. These risks are related to catastrophic changes. The natural disasters can be happened unexpectedly like flood fire etc.

2.3.3 Reasons for project failure in IT Industry

Different authors describe distinct reasons for project failure through different surveys and reports. A substantial number of projects fails in IT before coming to an end. For this reason, it has been a topic of great attention for many researchers. The basic reason for project collapsing is the confliction of interests of project members and the managers (Mahaney et al, 2003).

Keil et al (2004) depicted that a continuous unnecessary support from the managers after getting discouraging results from the projects. Then the projects will take more time to be finished than the specified period, which will eventually demand more resources like budgeting. It would be totally wastage of resources and a huge shortfall for an organization. (Chulkov et al, 2005). In 1997 KPMG International consulting firm identified three main and some other reasons for project failure, which are poor project planning, a weak business case, lake of top management involvement and support etc. (Whittaker, 1999).

Applegate et al (2009), holds responsible to IT and other management people for project failures on the of basis last ten years research and describes the following three main reasons.

a) Inability to apply certain risk management techniques before allocating resources to the project.
b) Inability to judge and accept to apply a collective risk management approach of a portfolio of projects.
c) Inability to know distinct project needs distinct approaches or methodologies to manage the project.

Implementation risk is described as something that will stay behind after using certain risk management techniques and methods i.e., mishandling could be another cause of risk which is not an integral part of the project. Moreover, some evaluations are comparatively easy before starting a project i.e., financial outcome, project cost, finishing date etc. but on the other hand some expectations could go wrong with the projects like time, cost estimation, technical deficiency etc. Ignoring this factor could be another big mistake and a reason of project failure. (Applegate et al, 2009).

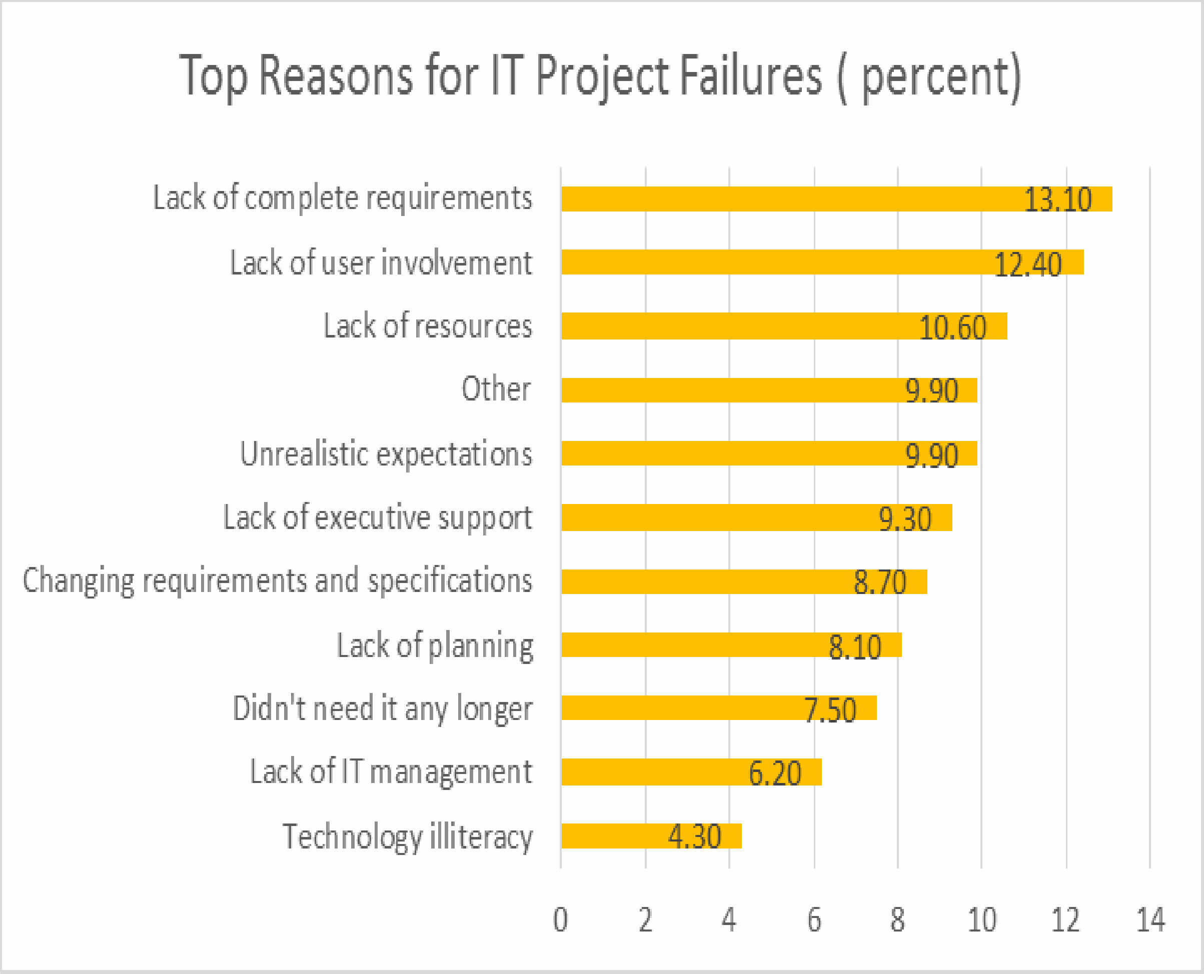


Figure 4: Top Reasons for IT Project Failures

(Source: Staff, I.A. (2016), 3 Premium Ways To Prevent IT Project Failure)

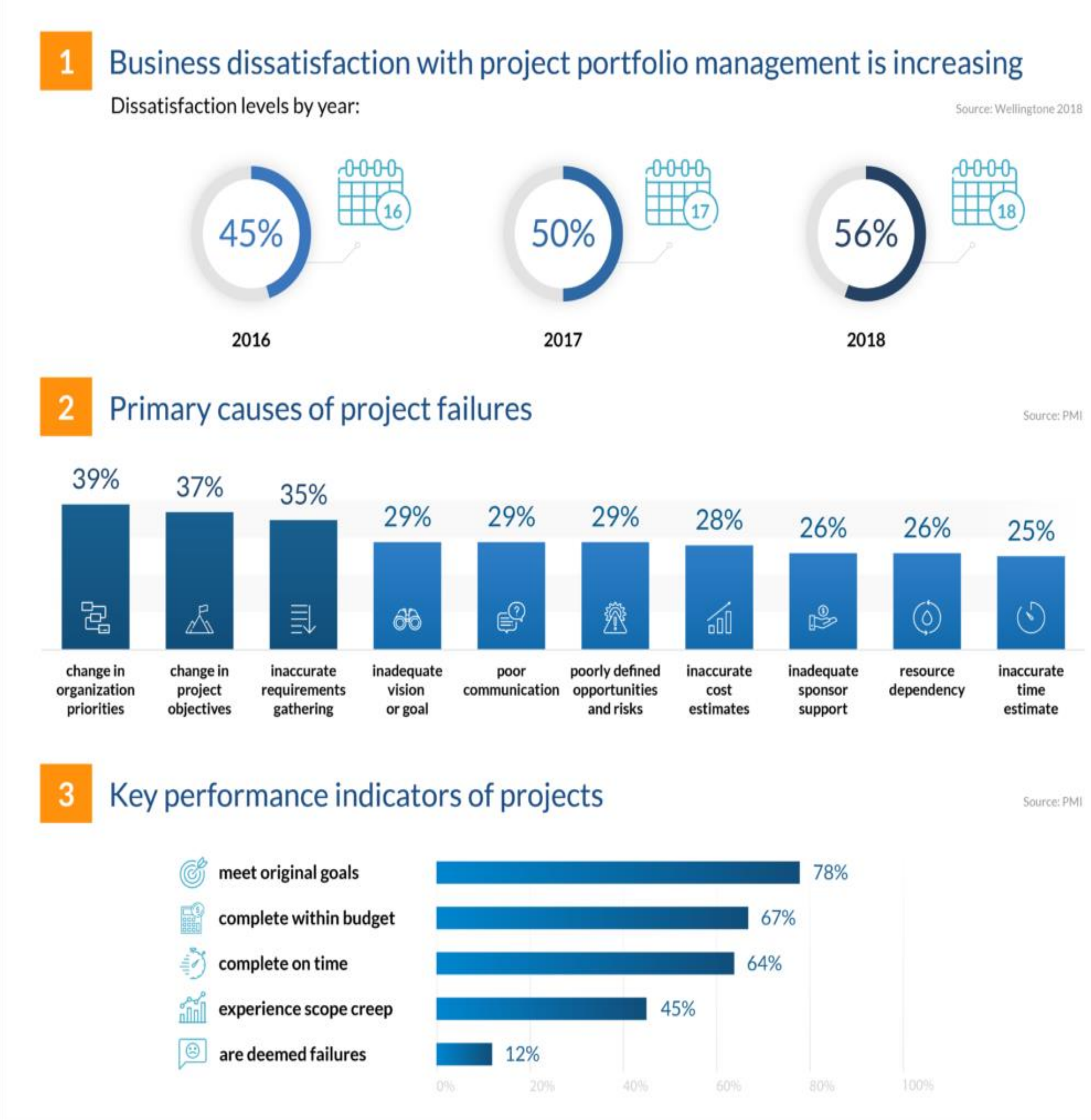


Figure 5: 3 Key Statistics

(Source: Gilbert, N. (2019), Project management software constantly evolves with the emerging technologies and approaches to planning budget)

2.3.4 Risk Identification

Identifying a risk has always been a challenge for organizations. It is the most critical reason for any project's success and failure. Managing a project is a challenging task because of the uncertainty and complexity to identifying the risks. When there is any mechanism of identifying the risk, it will make the project management task quite easy. There are many methods in practice for risks identification. Brainstorming technique (Mind Tools, 1996) is considered useful to collect the data of considerable number of risks while spending less time. Another method is known as Ishikawa (Kaoru Ishikawa, 1988), or cause- and-effect, diagram.

It is also known as fishbone diagram. This technique is used for quality analysis and to know about the causes of the problems. It can also be useful to use this with the brainstorming technique.

Another important technique for risk identification is checklist creation (Boeing, 1935). A checklist can be made from the past project management experiences which can provide a proper guideline for the project containing most usual risks. As all the project's solutions are based assumptions, so assumption analysis is used to analyze whether the project solutions assumptions are correct or not. (Taylor, 2004).

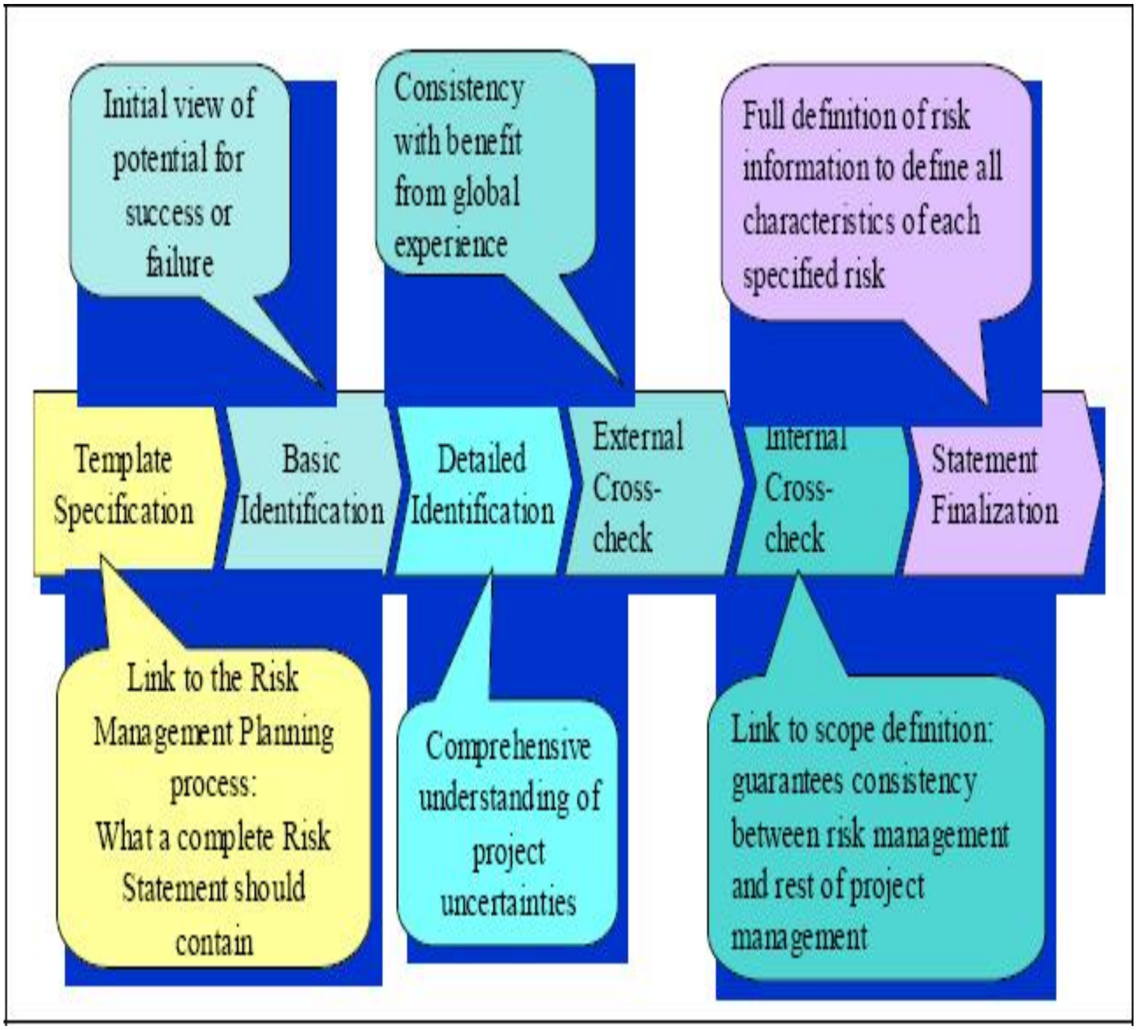

Initial view of potential for success or failure
Consistency with benefit from global experience
Full definition of risk information to define all characteristics of each specified risk
Template Specification
Basic Identification
Detailed Identification
External Cross-check
Internal Cross-check
Statement Finalization
Link to the Risk Management Planning process: What a complete Risk Statement should contain
Comprehensive understanding of project uncertainties
Link to scope definition: guarantees consistency between risk management and rest of project management

Figure 6: The six phases of the Risk Identification Lifecycle

(Source: Piney, C. (2003), Risk identification: combining the tools to deliver the goods)

2.3.5 Risk Theory 1

Applegate et al (2009) considered that risk is the vital part of business. The higher the risk taken in business, the higher would be return. Applegate et al (2009) further explains the implementation risk factors and classify them into three categories of risk factors.

a. Project size

Project size effect the risk factor. When a project size would be large in cost, time duration and number of departments involved in the projects then the risk will also be high.

b. Experience with technology

Unfamiliar technologies for IT personnel and other staff in the organization will increase the risk for projects. The projects exploiting modern technologies are at higher risks than the projects involved familiar technologies.

c. Requirements Volatility

Some projects are easy to manage because the outcome of the project can be clearly defined. In contrast, some projects have unsteady prerequisite. Volatility in projects requirements and changing nature of the project make it difficult to manage.

The project with enormous size, high use of unfamiliar technologies, and high requirement volatility factors are at higher risks. The project having two from the above-mentioned factors would be twice riskier than the project having one of the above factors.

2.3.6 Risk Theory 2

Whittaker, B. (1999) talks about a survey conducted in April 1997, a questionnaire focusing on IT project management issues was sent to Canada's leading 1,450 public and private sector organizations. KPMG's 1997 Survey of Unsuccessful Information Technology Projects revealed that the three most common reasons for project failure are:

a. Poor project Planning

Insufficient risk management with a poor project planning. It is more applicable to those organizations which are growing with economy. That is why large and growing organizations should have more focus on this area.

b. A weak Business Case

IT systems should be built according to the business requirements. There should be perfect alignment between the IT systems and the business needs.

c. Lack of top Management involvement and support

Lack of commitment and participation among the projects team members and insufficient support from top management is also a cause of unsuccessful project. Moreover, it usually creates troubles even before the beginning a project.

Some other reasons described in survey were, time required to complete a project exceeds the estimated budget, usage of new untested technology, wrong evaluation and ambiguity at project planning phase and vender's incapability to contain the agreement.

2.4 Others Research

Like above findings, a huge amount of data is available from the past research which is extremely useful to identification of risks. Every researcher adopted their own way of explaining and categorizing the risks. According to (Keil et al, 2004) customer mandate, scope & requirement, execution, and environment are the main risk factors affecting the projects. (Chetterjee et al, 1999) considers Business, Communication, Resource, Technical and Sociological risk factors are import. Whereas (Elkington et al, 2000), also consider the Business Risk one of the Risk factors but also describing some other risk like Management, Procurement and Technical risks. According to (Miller et al, 2001) research, Market-related, Technical, and Institutional risks could be the critical risks factors. (Boehm et al, 2003) research tells us that Environmental, Plan-driven, and Agile risk factor can be significant risks factors. Similarly, (Hall, 2003), (Murthi, 2002), (Bannerman, 2008), and (Stewart, 2005) contribute as an enormous amount of risk factors and categories.

2.5 Risk Identification - a dilemma

Bannerman (2007) says checklist is a straightforward way to cope up with risk factors in projects, but it has some challenges. For example, check list can be varying regarding time, culture, different stakeholders. That is why checklist could be biased and limited in scope. Some stakeholders may identify and could rank differently which are not directly relevant to them. Therefore, it is difficult to identify full range of list especially when the research is based on same kind of stakeholder group. "Analytical frameworks" is a way; looking risk categories like technology, requirements etc. consists of many risk factors this will give a broader framing than the simple checklist.

The software engineering related organizations are very much emphasizing on internal project risk i.e., Design, develop but ignoring external aspects i.e., Politics, volatility in business requirements. (Murthi, 2002).

The latest change in research work of project's assessment and focusing on any approach which can be helpful in all situations. To find out the intangible assessment criteria for projects, the criteria and the relevant sub-criteria should be collected and grouped them in an organized manner. Then this structured hierarchy makes it easy to assess the impact of the criteria and sub-criteria and help in examining the estimation for projects. (Stewart, 2005).

The detail about risk assessment of important influencing factors, such as values, perceptions, and attitudes. Furthermore, the circumstances like politics, culture and analyst's background, psychology, wisdom etc. which can affect risk assessment. (Stewart, 2005).

2.6 Risk Management Practices

A rich literature is available describing the ways to mitigate project risks. Some of research is as follows.

Pennock et al (2002) suggested three questions which should be considered while managing risks.

a) What can be done and what options are available to reduce the chances of risks to manage a project. Find out the number of ways and accessible choices of decreasing risks.

b) What are the tradeoffs in terms of all costs, benefits, and risks among the available options? Some options could be cost effective while others can be of low cost. So, choose the best viable option that is most suitable to an organization in terms of available resources and the risks and benefits associated with it.

c) What is the impact of current decisions on future options? The decisions taken by an organization should not disturb the other system within the organization. Some decisions can increase or decrease the intensity of other critical or non-critical risks.

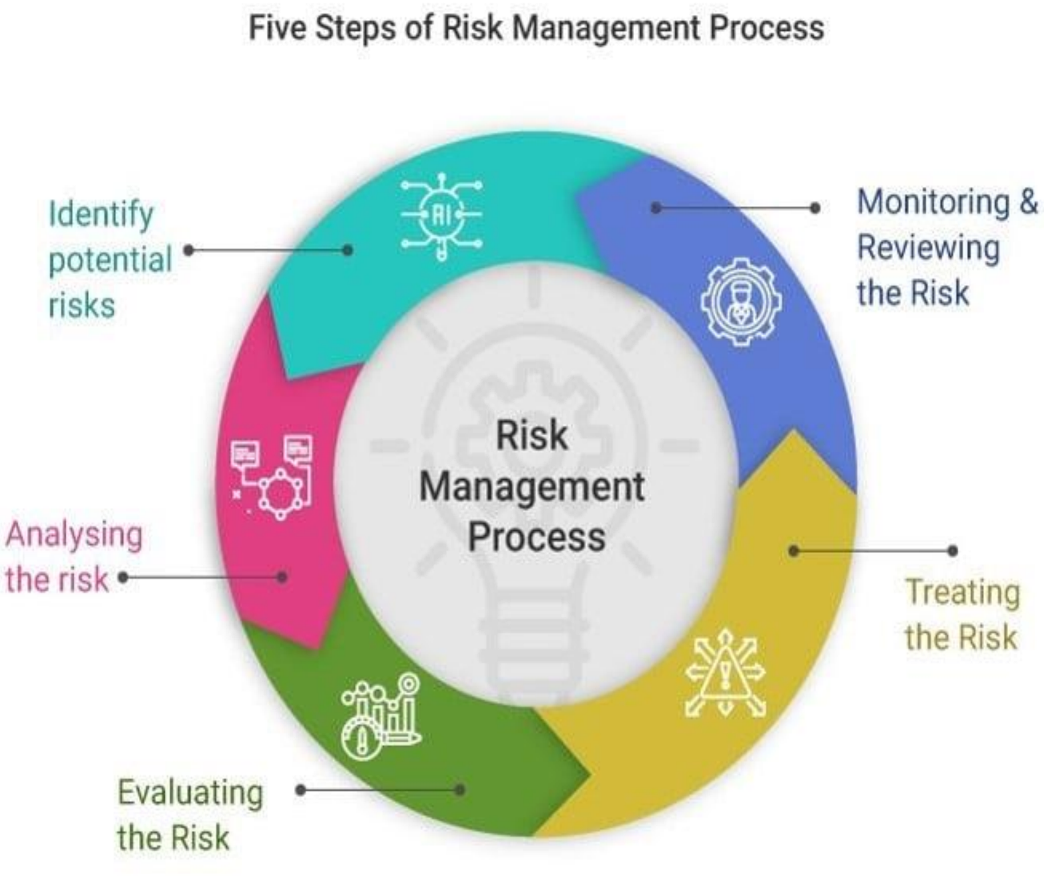


Figure 7: Risk Management Process

(Source: Brown, L. (2020), What is Risk Management in Project Management?)

Risk management is a software engineering practice with processes, methods, and tools for managing risks in a project. It represents a systematic approach to take initiatives to decide about the following tasks. (Samad et al, 2006).

a) A constant look on the project to observe if something happening inappropriate (monitor risks).
b) Prioritizing the risks to rectify them according to project requirements.
c) Apply proper methods and techniques to cope up with them.
d) At last, if still the risk is of high magnitude which is impossible to deal with available resources, then leaving the project in a condition that it may not affect the whole system. (Samad et al, 2006).

The management of the risk of project failures are based on the "spiral development model" which is very commonly used for software engineering practices. Boehm et al (2003) suggested two main steps to manage risks.

a) Risk Assessment
b) Risk Control

He further classified these two categories into more simplified and applicable steps and included three steps in each, Risk Assessment and Risk control.

Three main steps of Risk Assessment are Risk Identification, Risk Analysis and Risk Prioritization. In Risk Identification, Important risk factors are identified. In Risk Analysis, it determined that what could be the possible losses associated with these Identified Risk. Furthermore, In Risk Prioritization, identified risks are classified and place the substantial risk at the top of the list. Later, it is interpreted that the composite effect of the risk to facilitate the decision making, whether to keep on the project or stop the project even in middle. (Tiwana et al, 2006).

Moreover, further classification of "Risk Control" is related to Risk Management Planning, Risk Resolution and Risk Tracking or Monitoring (Samad et al, 2006).

2.7 Risk Response Strategies

A project Manager's methodology for managing the occurrence of risks events as termed risk response strategies (Taylor, 2004). Once risks have been identified and assessed, all techniques to manage the risk fall into one or more of these four major categories: (Dorfman, 2013).

a. Risk Avoidance

Attempting to structure and plan a project in such a way that it eliminates any threat or risk; usually by eliminating its causes is no way a feasible approach in terms of duration and cost. Similarly, there is not much worth and challenging in pursuing a project with no risk. Also, there are situations when a risk might lead to loss of time, revenues and even entire projects and not dealing with them properly is not wise either. Considering an alternative approach with less or no risks is the most followed practice. Insurable risks should be always avoided, if possible, by eliminating the cause of it.

b. Risk Acceptance

A risk which is expected and whose impact is within the level an organization can bear is accepted. There are situations when recourses become un-available or leave the organization. An organization acknowledges this risk as it is associated with every project and takes necessary measures in dealing with it when it occurs.

c. Risk Transference

Risks are transferred either by teaming up or by hiring a vendor. Hiring consultants or vendor companies, or by teaming up with other companies to gain the required expertise from them which the company does not have. Risk transference is also done by insurance for insurable risks such as hardware failure and fire. Consequences and responsibilities of managing risks are shifted to a third party.

d. Risk Mitigation

Mitigating a risk means reducing its impact or probability of its occurrence, or both. Adding cost or time for schedule, adding more experienced resources, using tried and test technologies are example of mitigating risk. Mitigating risk is also a form of accepting a risk, as the risk is expected and acceptable.

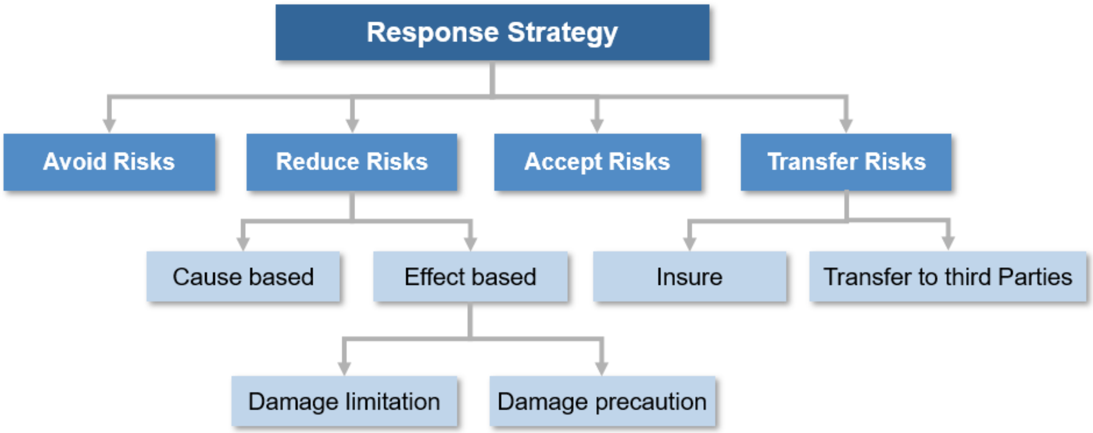


Figure 8: The different risk response strategies in response planning

(Source: Wanner, R. (2015), Project risk management: the most important methods and tools for successful projects)

2.8 Portfolio Approach for Risk Management

Portfolio risk management analyzes portfolio risk to reduce threats to a minimum or desirable level. The purpose is to reduce the negative impact of activities, events, and situations on a portfolio while also capitalizing on future possibilities.

Portfolio risk management is critical because of the considerable impact a component failure could have on a portfolio. The relevance of the portfolio is only highlighted by the fact that one portfolio component risk might potentially enhance the risk of others.

2.8.1 Portfolio Approach for IT risks

All IT risks are ended up as business risks. There is a need of an approach which can integrate IT risk into management of Business Risks. There are number of IT professionals to cope up with IT risks, but it is not essential that business managers should have knowledge about every activity running by IT professionals. There should be integrated IT risk management practice which can be undertaken by both IT professionals and business managers. This 'bridge of understanding' is known as IT portfolio management approach. It will provide the common conceptual umbrella to the business and IS research. In addition, building and updating the systems together with business related IT activities such as purchasing, procurement and outsourcing. This approach for managing IT risks is a way to integrate most critical IT risks and to manage them with the combine, organized and efficient manner. IT portfolio risks should be updated continuously keeping in mind the questions. i.e., what are the most significant IT risks, what techniques or methods must adopt to manage these risks, and who is going to manage these risks. (Jordan et al, 2005).

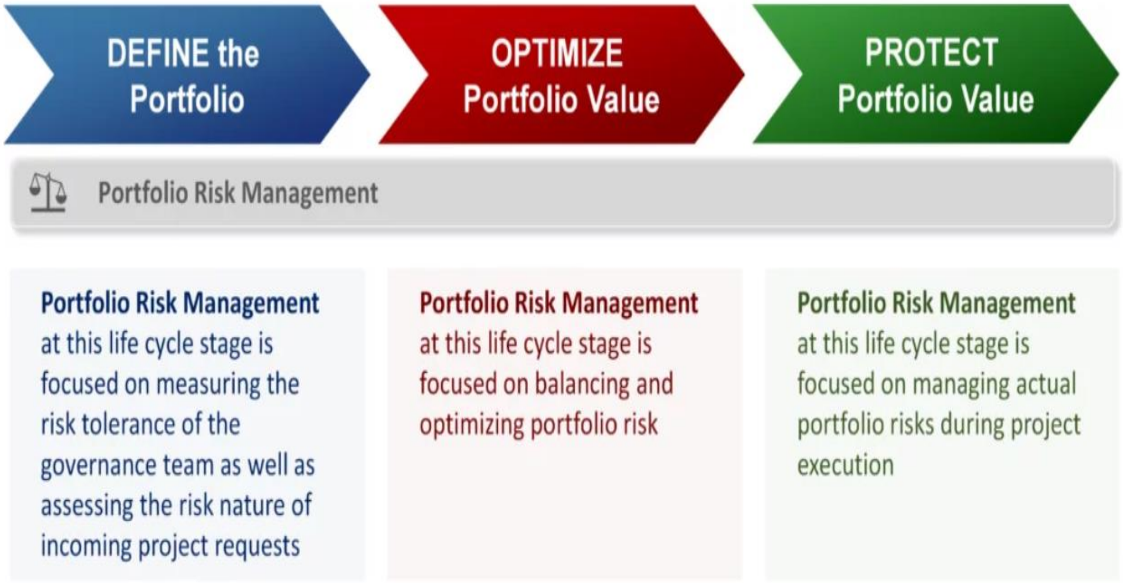

DEFINE the Portfolio
OPTIMIZE Portfolio Value
PROTECT Portfolio Value
Portfolio Risk Management
Portfolio Risk Management at this life cycle stage is focused on measuring the risk tolerance of the governance team as well as assessing the risk nature of incoming project requests
Portfolio Risk Management at this life cycle stage is focused on balancing and optimizing portfolio risk
Portfolio Risk Management at this life cycle stage is focused on managing actual portfolio risks during project execution

Figure 9: Portfolio Risk Management

(Source: Washington, T. (2020), PPM 101 - Portfolio Risk Management)

2.8.2 Project Portfolio Approach

The project portfolio is related to the process which already has infrastructure and investment to make changes happen. It provides number of ways to management to think about the project differently and to facilitate them in their decisions.

Information regarding the number of projects is gathered which could be related to budgeting, scheduling, projects benefit etc. it can be explained in two steps.

First, choosing a certain number of projects and secondly concentrating on a project critical factor. (Benko et al, 2003).

Economist Harry Markowitz introduced in 1950's the school of thought which we know as Modern Portfolio Theory.

"*Modern Portfolio Theory (MPT) says, in nutshell, that out of a universe of risky assets, an efficient frontier of optimal portfolios can be constructed that offers that maximum possible expected return for a given level of risk.*

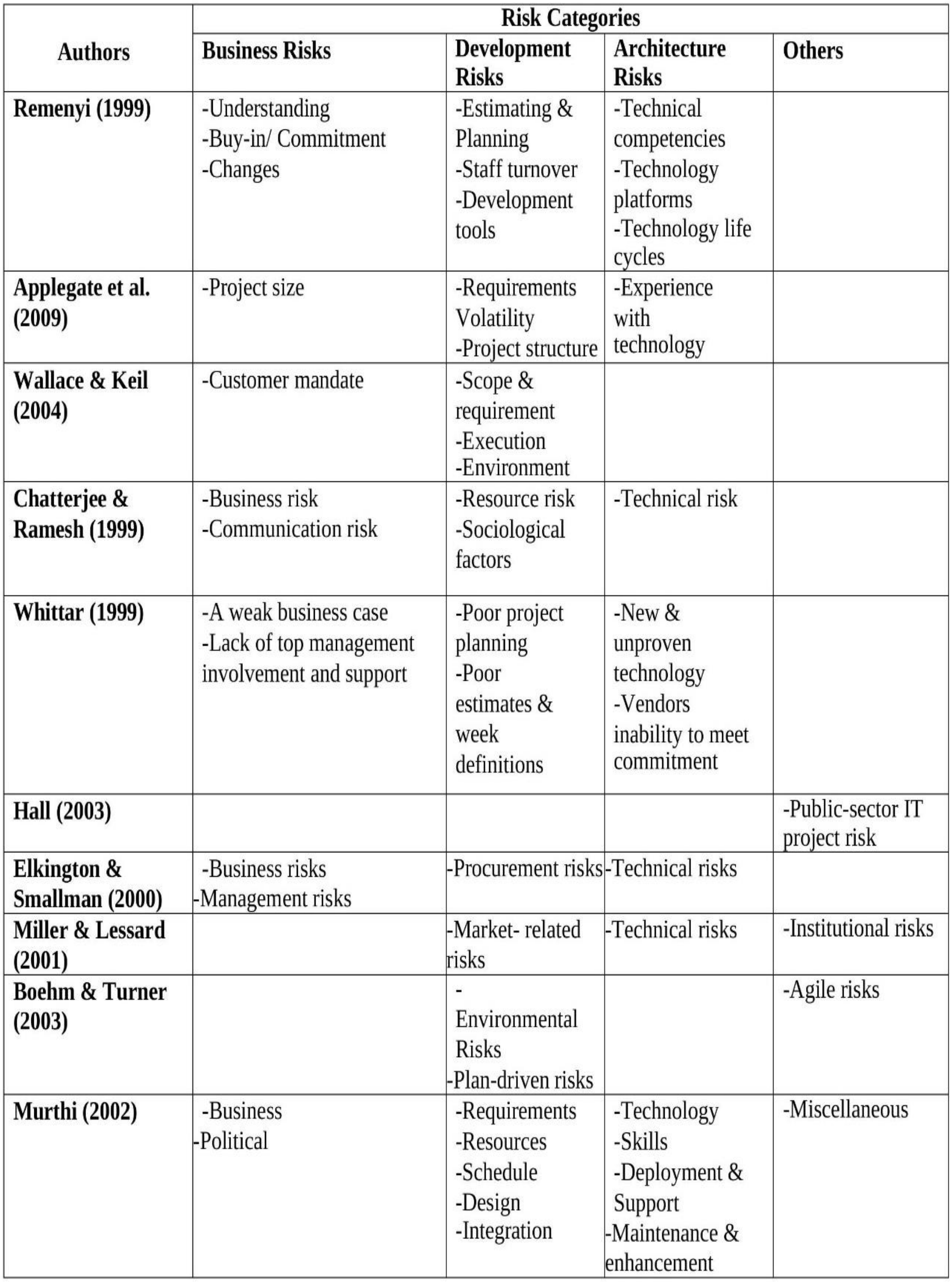
Modern Portfolio Theory argues that there is no single right portfolio. Rather, given the level of risk the investor wishes to bear and careful consideration of the combined value and risk of different assets within a portfolio, an efficient portfolio can be compiled to deliver the maximum benefit to that investor". (Benko et al, 2003).

2.9 My working definition of risk

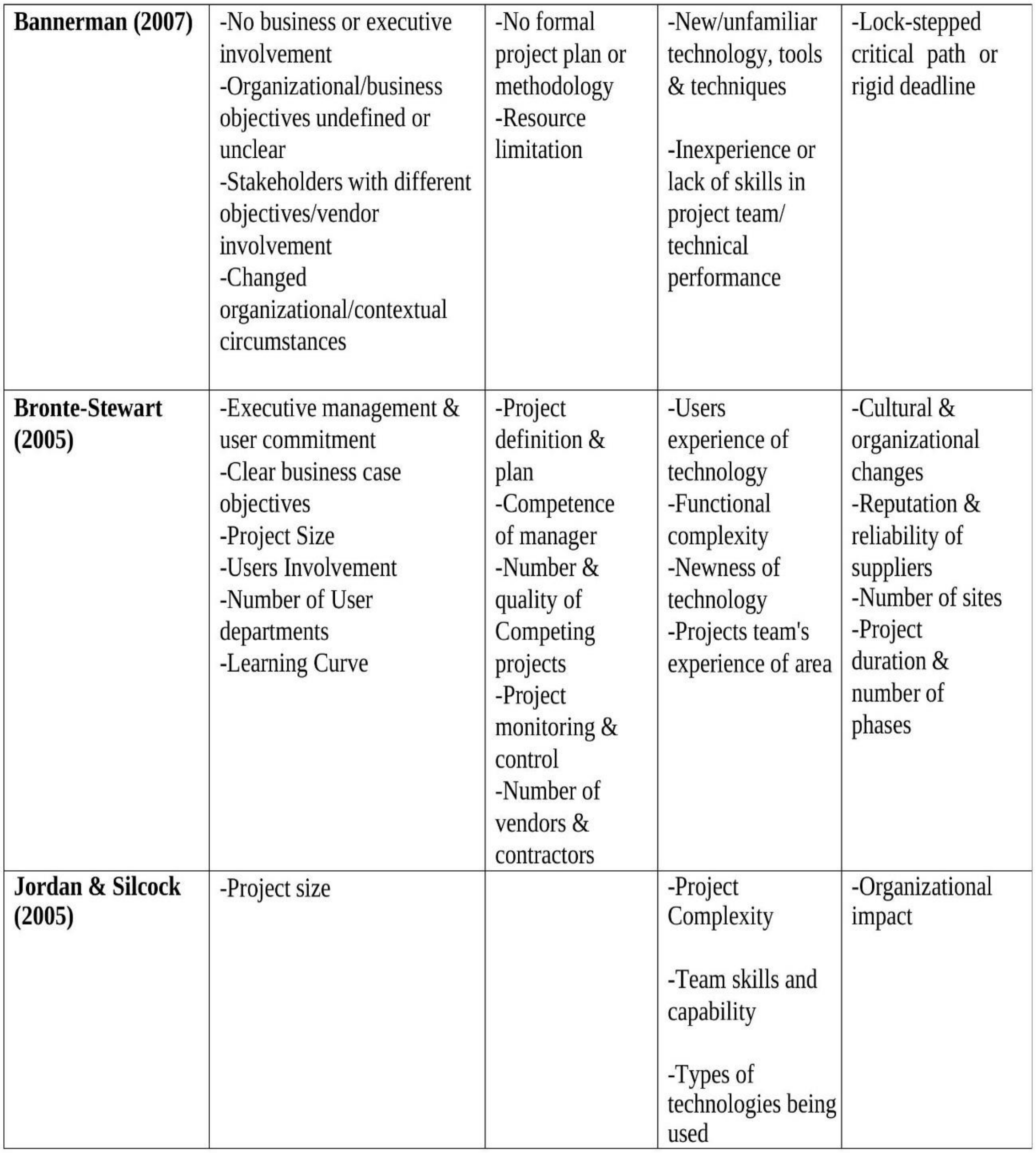
It is the possibility that during or at the start of a project, an unanticipated event can take place. The difference between the estimated and actual outcome indicates the degree/level of risk. Anything that could potentially impact project's timeline, performance, or budget. Any uncertain event or condition that, if it occurs, influences at least one project objective.

2.10 Summary of Literature Review

Based on the categorization of risks according to (Remenyi, 1999), we can place risk types mentioned by different noble authors. Following tables illustrates the categorization and further strengthens the choice of selecting Remenyi's approach for characterizing risks. Authors have used different names for types of risks, but we can see that majority of the risks fall under one of the three generic categories specified by Remenyi.



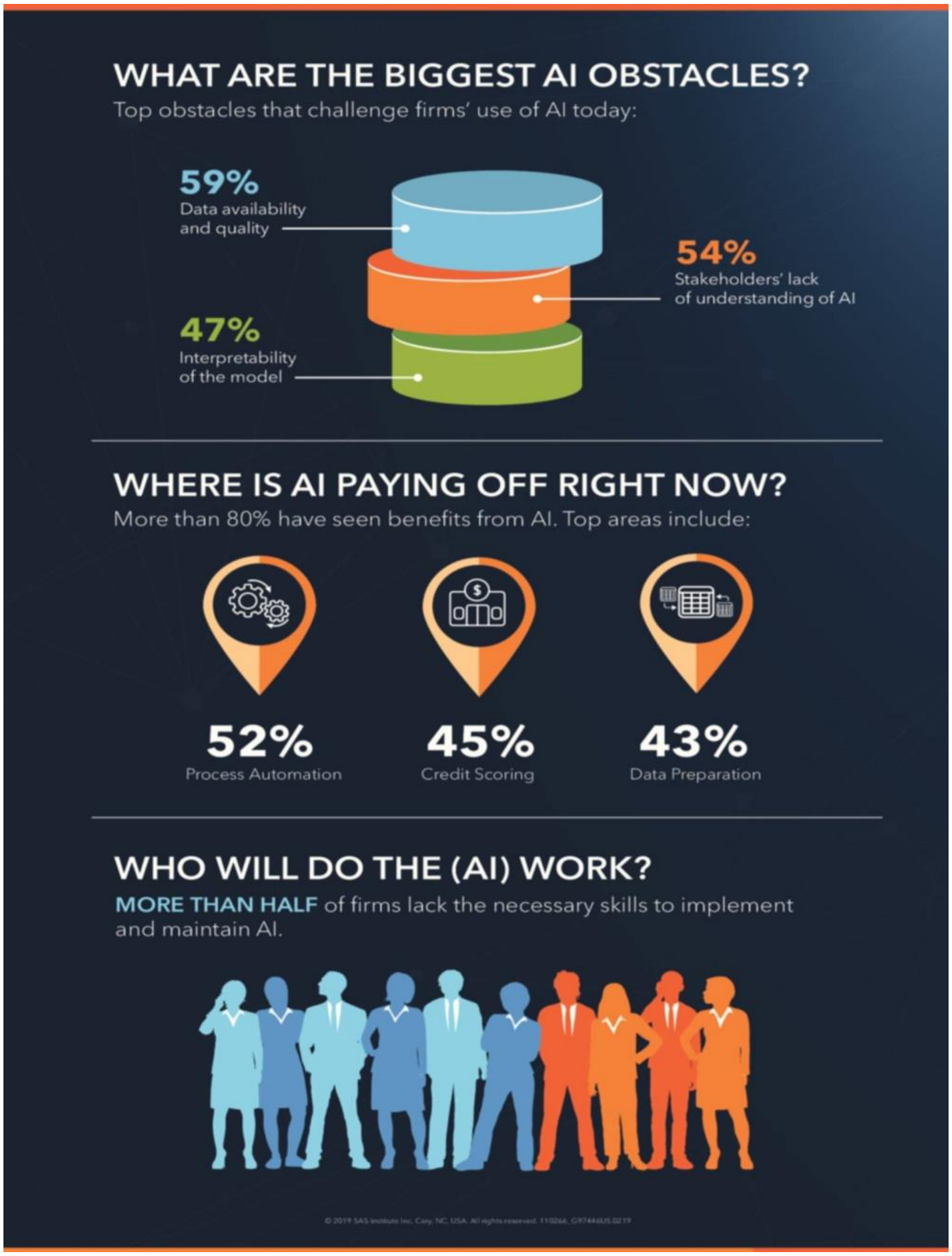
Authors	Risk Categories			
	Business Risks	**Development Risks**	**Architecture Risks**	**Others**
Remenyi (1999)	-Understanding -Buy-in/ Commitment -Changes	-Estimating & Planning -Staff turnover -Development tools	-Technical competencies -Technology platforms -Technology life cycles	
Applegate et al. (2009)	-Project size	-Requirements Volatility -Project structure	-Experience with technology	
Wallace & Keil (2004)	-Customer mandate	-Scope & requirement -Execution -Environment		
Chatterjee & Ramesh (1999)	-Business risk -Communication risk	-Resource risk -Sociological factors	-Technical risk	
Whittar (1999)	-A weak business case -Lack of top management involvement and support	-Poor project planning -Poor estimates & week definitions	-New & unproven technology -Vendors inability to meet commitment	
Hall (2003)				-Public-sector IT project risk
Elkington & Smallman (2000)	-Business risks -Management risks	-Procurement risks	-Technical risks	
Miller & Lessard (2001)		-Market- related risks	-Technical risks	-Institutional risks
Boehm & Turner (2003)		- Environmental Risks -Plan-driven risks		-Agile risks
Murthi (2002)	-Business -Political	-Requirements -Resources -Schedule -Design -Integration	-Technology -Skills -Deployment & Support -Maintenance & enhancement	-Miscellaneous



Bannerman (2007)	-No business or executive involvement -Organizational/business objectives undefined or unclear -Stakeholders with different objectives/vendor involvement -Changed organizational/contextual circumstances	-No formal project plan or methodology -Resource limitation	-New/unfamiliar technology, tools & techniques -Inexperience or lack of skills in project team/ technical performance	-Lock-stepped critical path or rigid deadline
Bronte-Stewart (2005)	-Executive management & user commitment -Clear business case objectives -Project Size -Users Involvement -Number of User departments -Learning Curve	-Project definition & plan -Competence of manager -Number & quality of Competing projects -Project monitoring & control -Number of vendors & contractors	-Users experience of technology -Functional complexity -Newness of technology -Projects team's experience of area	-Cultural & organizational changes -Reputation & reliability of suppliers -Number of sites -Project duration & number of phases
Jordan & Silcock (2005)	-Project size		-Project Complexity -Team skills and capability -Types of technologies being used	-Organizational impact

Table 1: Categorizing risks according to Remenyi

(Source: Remenyi, D. (1999), Stop IT project failure through risk management. Oxford: Butterworth Heinemann.)



WHAT ARE THE BIGGEST AI OBSTACLES?

Top obstacles that challenge firms' use of AI today:

WHERE IS AI PAYING OFF RIGHT NOW?

More than 80% have seen benefits from AI. Top areas include:

WHO WILL DO THE (AI) WORK?

MORE THAN HALF of firms lack the necessary skills to implement and maintain AI.

Figure 10: Current State & Future State on Artificial Intelligence in Risk Management

(Source: Carufel, R. (2019), 81 percent of risk management pros already seeing value of AI.)

2.11 Summary

A lot of researchers have divided IT risk management practices into two parts i.e., Risk assessment and Risk control. Risk assessment consists of three main actions, risk identification, finding out relevant possibilities and loss of the risks and ranking of those identified risks.

But there is a problem that risk assessment may not be same in all circumstances because the evaluation of risk is depending upon number of factors such as capability of an individual in terms of experience, risk perception. Moreover, checklist varies due to time, cultural, stakeholder differences, difference in background and more internal focus etc.

That is why it might be biased and limited in scope and may not contain full range of risks. Similarly, research can also vary due to individual's background, psychology, biasness, political reasons, and volatile requirements.

This factor can be minimized by providing a full range of list from real time data pulled with the help of artificial intelligence connect to actual data source which will give a more comprehensive set of risk factors which could be applicable in most of the circumstances. These identified risks can then be assessed to measure their impact on project management for IT industry.

As risks vary according to projects and organization, we can conclude Remenyi's approach of categorizing risk factors, leaving space for every organization to dig into risks as deep as they required. It is also a systematic way of understanding risk factors. These risk identification categories, which we can also be called as Gauges of a project can give number of advantages. These gauges will notify to executives and other management persons as well, who are not directly related to Information technology department, about the current position of the project.

Artificial Intelligence tools connected to Power BI[1] provide an unbelievably valuable approach for measuring the impact of risk factors in one view. In this way after identifying and categorizing risks, it can be measured that the project is at moderate, high, or extremely high degree of risks. Moreover, if we look at the level of risks in the perspective of my working definition, we can say when the project will be at its starting phase then the preemptive steps can be taken according to the measured level of risks. Whereas, when the project will be in progress the measured level of risk will be helpful in taking a proper responsive.

Using risk factors and categories by Remenyi and Applegate's for measuring risk impacts, we can get a better view of the projects which are at risk and different risks which might arise or hamper the project in future.

It is concluded that this structured approach is overall immensely helpful and gives many advantages which can be seen as listed below:

a) What could be the possible risk factors inherited in Projects. Gives a comprehensive list of risk factors from different researchers, background and culture, expertise etc. which are applicable to most of the circumstances.

[1] Power BI is a unified, scalable platform for self-service and enterprise business intelligence (BI). Connect to and visualize any data, and seamlessly infuse the visuals into the apps for everyday use.

b) Structured approach giving an in-depth and clear understanding of the risks associated with projects.

c) Helps organizations in prioritizing risky projects.

d) Deliver the same understanding for everybody without differentiating the IT professionals.

e) It distinguishes the various levels of risks i.e., moderate level risks, higher level risks etc.

f) As everybody can get the same understanding, there are very less chances of conflict while deciding. Conflicts can be raised when a project is at elevated risk level for one person but at the same time it could be at lower level for another person.

g) Helps in facilitating the top management while making the decision.

It not only helps in project management but also unbelievably valuable for an organization. This approach can be beneficial in changing organizational culture, where both technical and non-technical professionals are working together to confront the problems of project Management since it gives an understanding of risk impact for everyone.

This factor can be minimized by providing a full range of list from real time data pulled with the help of artificial intelligence connect to actual data source which will give a more comprehensive set of risk factors which could be applicable in most of the circumstances. These identified risks can then be assessed to measure their impact on project management for IT industry.

CHAPTER III:
METHODOLOGY

3.1 Overview of the Research Problem

The research question addressed in this study is the need to improve risk assessment in project management in the IT industry. As IT projects become more complex and critical to an organization's success, effective evaluation plays an important role in reducing project failure, project completion and return on investment.

Traditional approaches to risk assessment in project management rely on guidelines and concepts that can often be ignored or fail to address emerging risks and changing project dynamics. This can lead to inadequate risk mitigation strategies, overspending, delays, and overall project failure.

To overcome these limitations, the benefits of using artificial intelligence (AI) tools for risk assessment in project management in the IT industry are increasingly recognized.

Artificial Intelligence tools can analyze large amounts of data, identify patterns, and monitor in real time, thus increasing the accuracy and effectiveness of risk assessment. By incorporating artificial intelligence into the risk assessment process, project managers can make more informed decisions, identify emerging risks early and implement necessary risk mitigation strategies.

However, despite its benefits, integrating Artificial Intelligence tools for risk assessment into project management is also problematic. These challenges may include data quality and availability, ethical and privacy concerns, integration with existing systems and processes, and assumptions. Understanding and resolving these issues is critical to IT business success and the use of Artificial Intelligence tools in risk assessment.

Therefore, the research question focuses on exploring the impact of using artificial intelligence tools for risk assessment in project management in the IT industry. This study aims to explore the benefits, challenges, and barriers of integrating Artificial Intelligence into the risk assessment process. Addressing these research questions, this study focuses on the application of risk assessment, improving performance and driving innovation in the IT industry.

3.2 Operationalization of Theoretical Constructs

To apply the theoretical model in the research question, it is necessary to define and measure the relevant variables. Key theoretical constructs to be operationalized include:

3.2.1 Risk assessment using Artificial Intelligence tools:

Operational definition: Scope of project managers and IT professionals Adopt and use artificial intelligence tools for risk assessment in IT business management.

Performance Measurement: This can be measured through surveys or interviews to collect data on the frequency and extent of use of Artificial Intelligence tools, such as the percentage of jobs that use Artificial Intelligence tools for risk assessment, the type of Artificial Intelligence tools used. and the level of integration into projects in the management process.

3.2.2 Attitudes Towards Intelligence Tools for Security Assessment:

Operational Description: Positive or negative comments of project managers and IT professionals on the use of intelligence tools Intelligent for risk assessment in project management.

Functional assessment: Attitudes can be measured using questionnaire items based on the Likert scale, which indicate whether participants agree with statements about the positive, practical efficiency, effectiveness, and general understanding of intelligence tools for risk assessment.

3.2.3 Subjective Norms

Operational Description: Recognized community pressure or expectations to use Artificial Intelligence tools for risk assessment in project management.

Functional assessment: Key elements can be measured by asking respondents about their perceptions of stakeholders (e.g., colleagues, supervisors, customers) relevant to the use of Artificial Intelligence tools for risk assessment.

To consider or support the use of Artificial Intelligence tools in risk assessment, the assessment item will ask participants to what extent they perceive an impact on others.

3.2.4 Behavioral Intention

Functional Description: The readiness and willingness of project managers and IT professionals to use artificial intelligence tools for risk assessment in the risk management of the project.

Functional assessment: Attitudes can be assessed by asking respondents about their intention to adopt and use smart tools for workplace risk assessment in the future. This can be measured using a Likert scale-based survey item that achieves agreement with statements such as "I intend to include Artificial Intelligence tools for risk assessment in my future projects".

3.2.5 Actual Behavior

Functional Description: Specific actions taken by the project manager and IT professionals to adopt and use intelligence tools for risk assessment in process project management.

Functional assessment: actual behavior can be measured through participants' own reports or surveys, using artificial intelligence tools for risk assessment in project management. This may include collecting data on the frequency, duration, and scope of use of Artificial Intelligence tools and the benefits or effects of their use.

This identification and evaluation study allows the identification and evaluation of the main theoretical models involved in this study. By collecting data on these models, we can identify relationships between them, identify factors that influence the adoption and use of Artificial Intelligence tools, and explore their impact on the outcome of the IT industry.

3.3 Research Purpose and Questions

The purpose of this study is to examine the importance of using artificial intelligence (AI) tools for risk assessment in project management in the IT industry. This study aims to explore the benefits and challenges of integrating Artificial intelligence into the risk assessment process and its impact on outcomes. Addressing the limitations of traditional approaches and exploring the potential of expertise, this research focuses on the application of risk assessment and contributes to the improvement of management in the IT industry.

Research questions:

a) What are the limitations of risk assessment in project management in the IT industry?

b) How to Use Artificial Intelligence Tools to Improve Risk Assessment in Project Management in the IT Industry?

c) What are the benefits of using Artificial intelligence tools for risk assessment in the IT industry?

d) What are the challenges and limitations of integrating Artificial intelligence into risk assessment processes?

e) How does the integration of Artificial intelligence tools for risk assessment affect outcome in the IT industry?

f) What are the critical success factors for using Artificial intelligence tools to assess risk in the IT industry?

g) What are the implications of using Artificial intelligence tools for risk assessment in project management in the IT industry?

This research question provides a basis for exploring the importance of using Artificial intelligence tools for risk assessment in project management in the IT industry. They aim to assess the limitations of traditional methods, examine the benefits and challenges of Artificial intelligence integration, evaluate the impact of the event, and determine the importance of implementation and its impact on project management.

3.4 Research Design

The study will be using Contemporary research[2] methodology which combines quantitative and qualitative approaches to provide additional perspectives, create a richer picture and present multiple findings. The quantitative methodology provides definitive facts and figures, while the qualitative provides a human aspect. This can produce interesting results as it presents exact data while also being exploratory.

The research methodology for this study on using Artificial Intelligence tools for risk assessment in project management for the IT industry will involve the following steps:

a) **Theoretical framework**: The theoretical framework will be based on previous studies on risk assessment, project management, and AI tools. The framework will be used to guide the research process and provide a foundation for the research.

[2] *Contemporary research* means professional research studies that provide evidence of the impact of instructional practice and instructional leadership. Research findings are considered “contemporary” when conducted within the last ten (10) years or where the continued validity of less recent findings is supported by research conducted within the last ten (10) years.

b) **Research questions**: The research questions will be developed based on the research problem and the theoretical framework. The research questions will guide the data collection and analysis process.

c) **Data collection:** Data will be collected from various sources, including case studies, interviews, surveys, and secondary data sources. The data will be collected through survey from a pool of 53 practitioners in the field of project management and Artificial Intelligence.

d) **Data analysis**: The collected data will be analyzed using statistical analysis and machine learning algorithms. The analysis will focus on identifying patterns, relationships, and trends in the data, and the effectiveness of Artificial Intelligence tools in risk assessment.

e) **Results and discussion**: The findings of the analysis will be presented and discussed, including the benefits, limitations, and challenges of using Artificial Intelligence tools for risk assessment in project management for the IT industry. The results will be compared with existing literature and recommendations will be made for practitioners & future research by contributing to the body of knowledge.

f) **Conclusion**: A conclusion will be drawn based on the findings of the study, highlighting the implications and significance of the research for project management practitioners and researchers.

The research framework will be based on the principles of the scientific method, including observation, hypothesis testing, data analysis, and conclusion drawing. The framework will be used to systematically investigate the research problem and provide a rigorous and valid approach to the study.

The research methodology will be a mixed-method approach, involving both qualitative and quantitative methods to gather data and analyze the effectiveness of Artificial Intelligence tools for risk assessment in project management.

3.5 Population and Sample

The population of this study is project managers who take part in project management and risk processes and IT professionals working in the IT industry. This includes people from various organizations such as project managers, team leaders, risk managers, executives and other stakeholders involved in project management and risk assessment in the IT industry.

Sample:

Due to the large population and diversity, the sample of participants will be chosen to represent the larger population. The sample is chosen based on how it represents the population and provides insight into the research question.

Sampling techniques such as stratified sampling or random sampling will be used to select participants from various teams, business units and various types of projects.
The sample will include a variety of experts with varying levels of experience, expertise and responsibilities in project management and risk assessment.

It is important to ensure a sufficiently large sample size for meaningful analysis and generalization of results. The size will depend on factors such as design, data collection and statistical power.

Additionally, for risk assessment in project management in the IT industry, it will be helpful to consider a target sampling or snowball example to identify and include participants' knowledge or skills in using Artificial Intelligence tools. This will help ensure that the sample includes individuals with prior knowledge and understanding of Artificial Intelligence integration tools.

Care will be taken to maintain ethical considerations, such as obtaining informed consent from participants, keeping information private and confidential, and following ethical principles for research involving human subjects.

By choosing an appropriate model, we can gather insights and perspectives from managers and IT professionals involved in project management and risk assessment in the IT industry. This will provide key insights to solve research questions and lead to a deeper understanding of the importance of using Artificial Intelligence tools for risk assessment in the context of the IT industry.

3.6 Participant Selection

Selection of participants for research is based on research objectives and specific criteria that meet the research questions and sample requirements. Some aspects in selecting participants are:

A. **Inclusion Criteria**: Identify specific characteristics and qualities that participants must possess to be effective for the study. This may include factors such as roles in project management and risk assessment, experience levels, work history, and knowledge of Artificial Intelligence tools.

B. **Sampling Techniques**: Select the appropriate sample based on population and design. Stratified sampling, random sampling, or a combination of both will be used to provide a representative sample from the various teams, business units, and types of projects within the unit.

C. **Sample size**: Determine the required sample size based on factors such as statistical power, feasibility, and scope of work. Larger samples may provide stronger findings, but it is important to have a balance between appropriate sample size and available resources for data collection and analysis.

D. **Recruitment Process**: Review the qualifications and procedures required for recruitment. This will include reaching out to professional organizations, networking events, online communities and connect with potential participants who meet the criteria, including the standard.

E. **Informed Consent**: Obtain informed consent from participants before participating in the study. Clearly state the purpose of the study, the data collection process, the privacy measures, and the risks or benefits associated with participation. Participants should be able to choose to refuse or withdraw from the study at any time.

F. **Diversity and representation**: Try to provide diversity in the selection of participants to better understand the research question. It is designed to include individuals from a variety of business units, backgrounds and experiences using Artificial Intelligence tools for risk assessment. This will help capture more perspectives and improve the generalizability of the findings.

G. **Data Saturation**: Think of data saturation as an adequate determination of sample size. Data saturation is reached when new information or insights are no longer emerging from the data collection. If data saturation is reached before the criterion sample size is reached, this may indicate that sufficient data has been collected and that further research is not needed.

By carefully selecting participants based on these assumptions, we can ensure that the sample is representative, diverse, and aligns with research objectives. This will increase the effectiveness and reliability of research studies and allow for a comprehensive review of the importance of using Artificial Intelligence tools for risk assessment in management project in the IT industry.

3.7 Instrumentation

Instruments are tools or instruments used to collect data in research. In the context of current research, some of the tools that will be used for data collection are:

A. **Surveys/Questionnaires**: Surveys can be designed to gather information from participants about the use of Artificial Intelligence tools for risk assessment, the behavior of Artificial Intelligence integration, design, subjective norms, behavior, and Perceived outcomes. Likert scale items, multiple choice questions will be included in the survey tools to get answers from the participants.

B. **Interviews**: Model interviews or semi-interviews can provide valuable insights into participants' experiences, perceptions, and understandings of the use of an Artificial Intelligence tool for risk assessment. Interview questions will be designed to explore the effectiveness of Artificial Intelligence tools, challenges encountered, perceived benefits, and suggestions for improvement.

C. **Focus Groups**: Holding discussions with project managers can facilitate group discussion and understanding of the importance of using artificial intelligence tools for risk measurement. Group meetings can explore participants' perspectives, spark discussion on key issues, and uncover shared experiences and insights.

D. **Case Study**: Conducting a case study will involve using a variety of data collection methods such as interviews, observations, data analysis and data collection. This comprehensive guide provides information on the uses, challenges, and benefits of integrating Artificial Intelligence tools for risk assessment into a project or organization.

E. **Observations**: The observation process will be used to collect data on the actual use and impact of Artificial Intelligence tools for risk assessment in project management. This will include monitoring participants' interactions with Artificial Intelligence tools, their decision-making processes, and the validity of risk outcomes.

F. **Document Analysis**: Analyzing relevant documents such as project documentation, risk assessments, and project management procedures can provide valuable insights for risk assessment. This helps to understand current practices, identify gaps, and evaluate the role of Artificial Intelligence in improving risk assessment.

G. **Existing data source**: Depending on the context, existing documents such as organizational documents, project management documents, and background documents will also be used to collect data on the use of Artificial Intelligence tools to assess the risks and benefits of the project. These secondary data can complement the primary data collection process.

The choice of tools will depend on the research question, the design, and the type of data needed to effectively address the research question. It is important to ensure that the tool is effective, reliable, and suitable for capturing the variables and patterns of interest. Testing and verification procedures will be performed to ensure that the device measures the correct design and produces reliable data.

3.8 Data Collection Procedures

The data collection process will include the following steps:

A. **Define data collection plan**: Identify specific data collection methods, tools, and techniques to use Research Design.

B. **Obtaining ethical approval**: Obtaining ethical approval from the institutional review board or ethics committee to ensure that the research is ethically appropriate and to protect the rights and privacy of participants.

C. **Participant Recruitment**: Recruitment according to participant selection. Engage with participants through networks, organizations, online communities, or other appropriate channels. Provide clear information about the study and obtain informed consent from participants.

D. **Pretest/Pilot Test**: Perform a pretest or pilot test phase to assess the quality and clarity of the data collection tool. This includes testing the tool with a small group of participants and making any necessary adjustments to ensure validity and reliability.

E. **Data Management**: Organize and securely store the collected data, ensuring confidentiality and privacy. Implement appropriate data management procedures, including anonymization and coding of participant information for confidentiality purposes.

Throughout the data collection process, will communicate with participants, address any concerns or questions they may have, and ensure the confidentiality and anonymity of their information. Be ethical and protect the rights and well-being of participants throughout the data collection process.

3.9 Data Analysis

Data analysis is an important step in the research process, which involves transforming collected data into meaningful insights, patterns, and conclusions. Some data analysis methods that will be used are:

3.9.1 Quantitative data analysis:

A. **Descriptive data**: Calculate and analyze descriptive data such as mean, pattern difference, frequency, and percentage, or search for Quantitative data from the survey to conclude and explain research results.

B. **Inferential Statistics**: Investigate relationships or differences between variables using inferential statistical methods such as correlation analysis, regression analysis, t-test, ANOVA, or chi-square test.

C. **Factor Analysis**: Perform an analysis to identify dimensions or characteristics in a group of variables related to intellectual property, risk assessment, project outputs, or other structures.

D. **Data Mining Techniques**: Use data mining techniques such as clustering or classification algorithms to identify patterns or classify data by features or characteristics.

3.9.2 Qualitative Data Analysis:

A. **Thematic Analysis**: Use thematic analysis to identify and identify recurring themes, patterns, or trends in qualitative data from interviews, focus groups, or open-ended responses.

B. **Content Analysis**: Perform content analysis to classify and analyze information from documents, reports or other written sources related to Artificial Intelligence integration, risk assessment or project management.

C. **Coding**: Use coding techniques such as open coding, axial coding, or selective coding to classify and organize qualitative data into themes for analysis.

D. **Narrative Analysis**: Analyze narratives and stories in qualitative data to understand participants' experiences, thoughts, and feelings about using Artificial Intelligence tools in risk assessment.

3.9.3 Mixed Method Analysis:

A. **Integration of Quantitative and Qualitative Data**: Combining and analyzing quantitative and qualitative data for a comprehensive understanding of research questions. Strategies of triangulation, complementarity, or continuum can be used to optimize the quality of the two types of data.

B. **Data Visualization**: Effectively present meaningful data using charts, graphs, tables, or other visual representations. Data visualization techniques can help identify patterns, patterns, and relationships in data.

C. **Interpretation and Synthesis**: Interprets and synthesizes data to answer research questions, state research objectives, and draw conclusions. Relate research findings to existing literature, theories, and concepts to provide insight and contribute to knowledge in the field.

It is important to ensure the rigor and reliability of the data analysis process by using appropriate software tools, performing reliability tests of the auditor's review, controlling the analysis of decisions, and seeking advice or opinions from peers or experts. To increase analytical validity.

3.10 Research Design Limitations

Study design limitations are limitations or deficiencies that may affect the validity, efficacy, or reliability of the study. In the context of using Artificial Intelligence tools for risk assessment in project management in the IT industry following are some of the potential limitations:

Sample bias: Some demographic, organizational, or industry-specific characteristics may not be well captured in the sample, limiting the generalizability of the findings.

Self-Reported Data: This research may be based on self-reported data obtained through surveys, questionnaires, or interviews. Participants may provide misleading or inaccurate information due to memory recall issues, social desirability bias, or misinterpretation.

We should recognize the limitations of self-reported data and consider triangulating it with other data or methods.

Cross-sectional design: If the study design is cross-sectional, it captures information of specific points in time. This design limitation may limit the ability to create relationships or view changes over time. Attempts to design longitudinal studies or control groups can provide strong evidence for causation but may be constrained by logistical constraints or constraints.

Potential differences: There may be other or different factors that are not fully controlled or considered in the study design that may affect the results of the risk assessment using Artificial Intelligence tools in project management. These inconsistencies may cause bias or affect the interpretation of results.

Generalizability to other businesses: Findings may be specific to the IT industry and have limited applicability to other businesses or industries. Different industries may have unique characteristics, risk profiles, or project management that can affect the feasibility and effectiveness of using Artificial Intelligence tools for risk assessment.

Technological Advances: The findings and conclusions of this study will be limited to the rapid development of Artificial Intelligence technology and tools. According to the technology, the state of artificial intelligence equipment at the time of research may be more or less beneficial, which may affect the generality and applicability of the research in the future.

Limitations of Artificial Intelligence tools: This study may encounter limitations with certain Artificial Intelligence tools used to assess project management risk. These limitations may include already existing algorithmic bias, data quality issues, inadequate interpretation of Artificial Intelligence -generated results, or issues of integrating Artificial Intelligence tools into project management processes.

To understand the possibilities, biases, and limitations of research, it is important for to openly acknowledge and discuss the limitations of research design. Addressing and reducing these limitations as much as possible can help increase the precision and reliability of research studies.

3.11 Conclusion

Research methodology play an important role in the study of risk assessment using artificial intelligence tools in project management in the IT industry. The chosen methodology guides the overall research process, including the selection process, study purpose, questions, design, participant selection, data collection methods and procedures. By carefully planning and implementing research, we can define research objectives, produce reliable and valid data, and draw conclusions.

Quantitative, qualitative, or mixed research design should be consistent with the research questions and objectives. It is important to select appropriate tools and data collection methods to collect important and reliable data from the target population.
The sample selection process should be rigorous and objectively diverse to improve the representativeness of research results. Data analysis techniques such as statistical analysis, thematic analysis or content analysis should be used to analyze the collected data and draw conclusions.

However, it is important to acknowledge the limitations of the research methodology. Sample bias, self-reported data, cross-sectional design, potential confounding variables differences between variables, general limitations, and rapid development of AI systems are some of the limitations that need to be considered. By addressing these limitations and being clear about them, we can ensure the reliability and validity of their research findings in the areas they describe.

Finally, a well-planned and well-executed research process can explore the importance of using Artificial Intelligence tools for risk assessment in project management in the IT industry. It provides a solid foundation by generating valuable insights in the IT industry, contributing to knowledge, and informing decision-making processes.

CHAPTER IV:
RESULTS

4.1 Introduction

The purpose of this section is to present and discuss the main results obtained in the study on the use of artificial intelligence tools for risk assessment in project management in the IT industry. The survey aimed to gather information from project managers & executives about their experience, insights, and challenges in integrating Artificial Intelligence tools for risk assessment.

In this section, we describe the methodology, including sample size, participants, and data collection procedures. Next, we practice analyzing the answers to the questions by highlighting the main themes and patterns that appear in the data.

Survey responses were collected from an online survey distributed to a group of 53 executives and project managers in the IT industry. The survey consisted of a combination of closed and open-ended questions that allowed respondents to provide quantitative assessments and recommendations on various aspects of risk assessment through Artificial Intelligence tools.

Analysis of survey data included both descriptive statistics such as frequencies and percentages, and thematic analysis of open-ended responses. The survey results are designed to better understand the participants' perspectives and experience in using Artificial intelligence tools for risk assessment in project management.

In the following sections, we present the results of the analysis in detail and structure, highlight the main findings, discuss their conclusions, and provide relevant evidence from the comments.

4.2 Survey Result

(Sample = 53 Project Managers / Executives)

4.2.1 Research Question One: On a Likert scale from 1 to 5, where 1 represents "None" 2 (Basic) 3 (Intermediate) 4 (Advanced) and 5 represents "Expert"

Please, rate the level of your received training in risk management in your company.

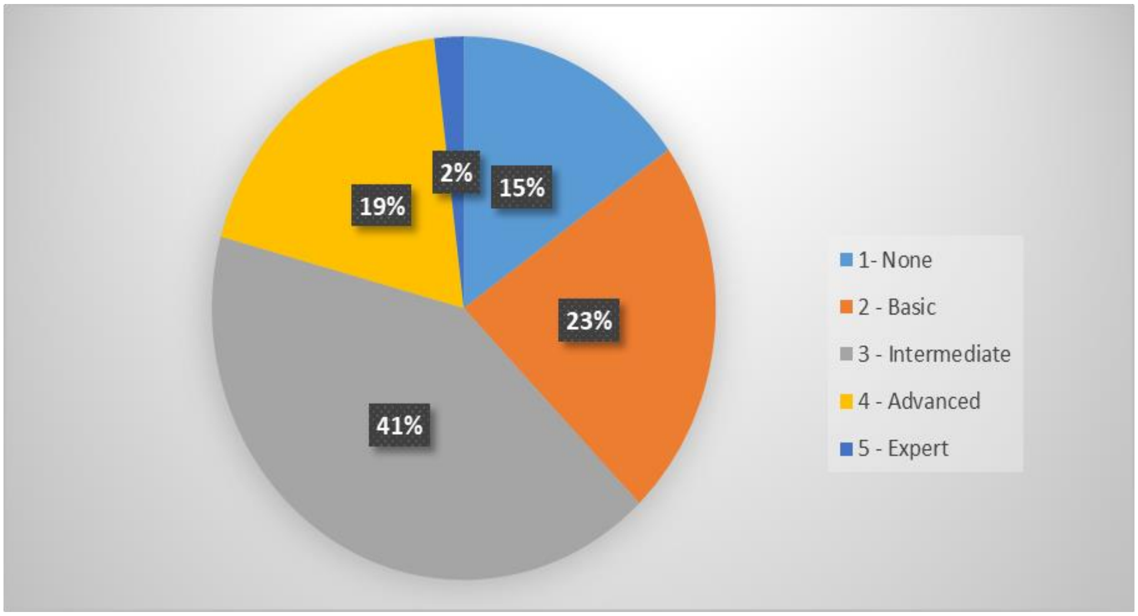


Figure 11: Level of Training in risk management

Significant proportion of respondents (15%) reported receiving no training in risk management within their company. The majority of respondents (42%) indicated that they have received intermediate level training, while 23% reported basic level training. A smaller percentage of respondents (19%) mentioned having advanced level training in risk management, and only 2% considered themselves as experts in this area.

4.2.2 Research Question Two: On a scale of 1 to 5, where 1 is "Strongly Disagree" and 5 is "Strongly Agree" please rate the following statements regarding your team's assessment of risk management and prioritization of risk management activities:

Our team has a clear understanding of risk management principles and practices.

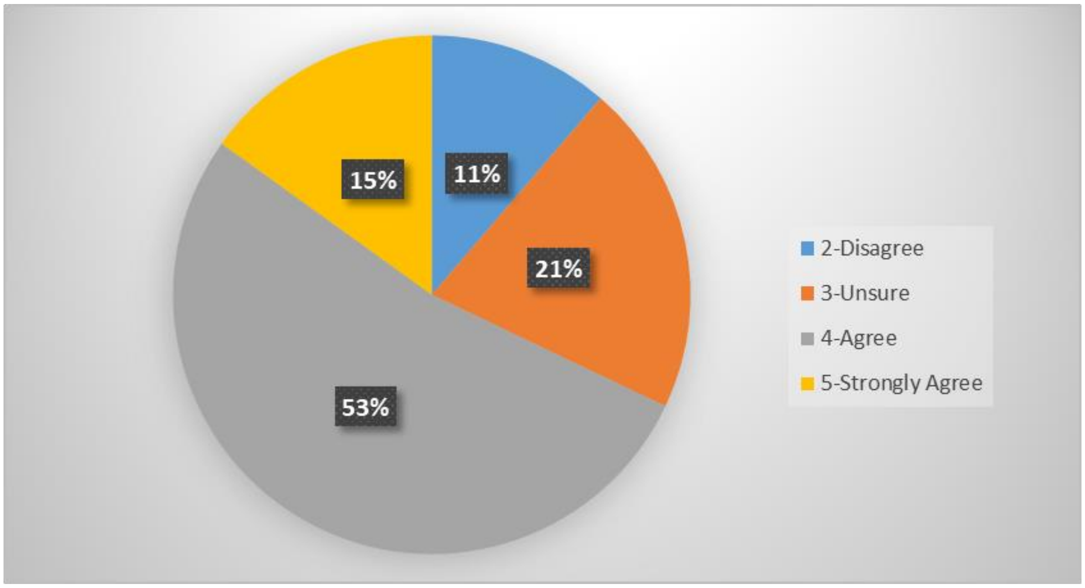


Figure 12: Understanding of risk management principles and practices.

Majority of respondents (53%) agreed that their team has a clear understanding of risk management principles and practices. A significant portion of respondents (21%) were unsure about their team's understanding, while a smaller percentage of respondents (11%) disagreed with the statement. Additionally, 15% of respondents strongly agreed that their team has a clear understanding of risk management.

4.2.3 Research Question Three: On a scale of 1 to 5, where 1 is "Strongly Disagree" and 5 is "Strongly Agree" please rate the following statements regarding your team's assessment of risk management and prioritization of risk management activities:

Our team effectively assesses risks and identifies potential issues.

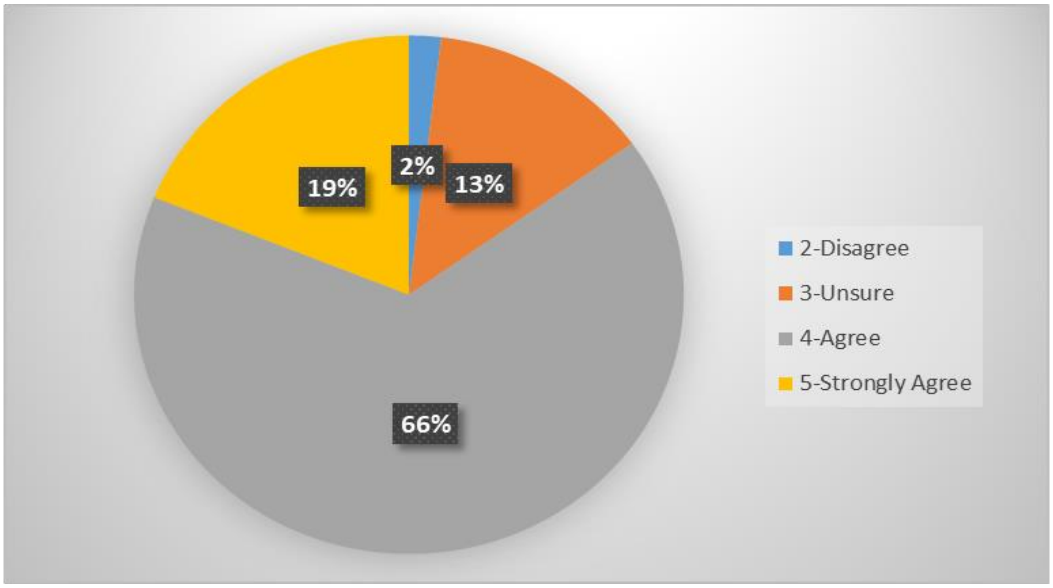


Figure 13: Effectively assessing risks and identifying potential issues.

Significant majority of respondents (66%) agreed that their team effectively assesses risks and identifies potential issues. A notable percentage of respondents (19%) strongly agreed with the statement. However, a small percentage of respondents (2%) disagreed with the statement, and 13% expressed uncertainty.

4.2.4 Research Question Four: On a scale of 1 to 5, where 1 is "Strongly Disagree" and 5 is "Strongly Agree" please rate the following statements regarding your team's assessment of risk management and prioritization of risk management activities:

Our team has a clear process for prioritizing risk management activities.

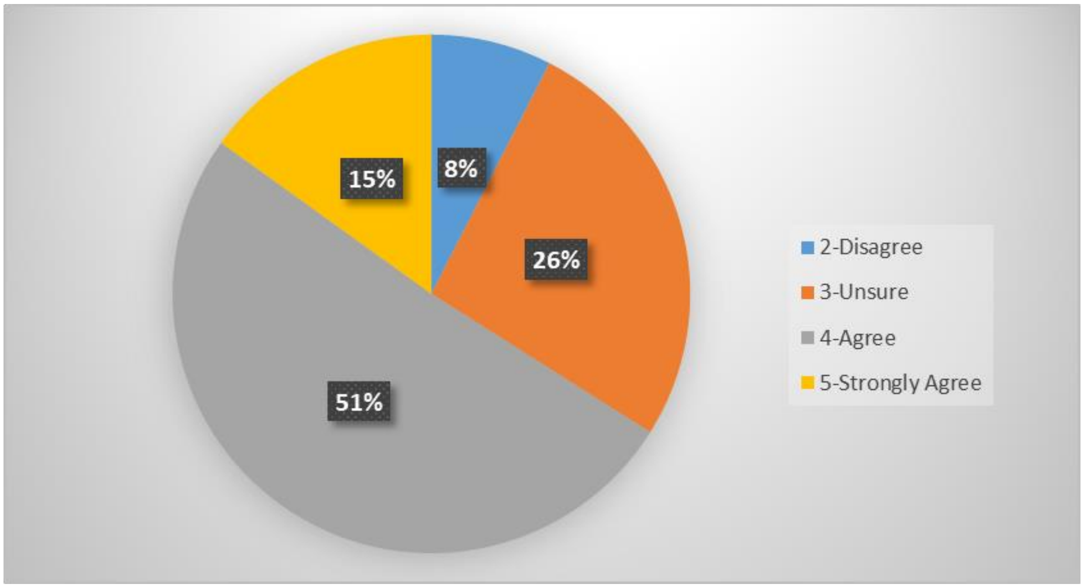


Figure 14: Clear process for prioritizing risk management activities.

Majority of respondents (51%) agreed that their team has a clear process for prioritizing risk management activities. A smaller percentage of respondents (15%) strongly agreed with the statement. However, a notable proportion of respondents (26%) expressed uncertainty about their team's clarity in prioritizing risk management activities, and a small percentage (8%) disagreed with the statement.

4.2.5 Research Question Five: On a scale of 1 to 5, where 1 is "Strongly Disagree" and 5 is "Strongly Agree" please rate the following statements regarding your team's assessment of risk management and prioritization of risk management activities:

Our team consistently implements risk management strategies to mitigate potential risks.

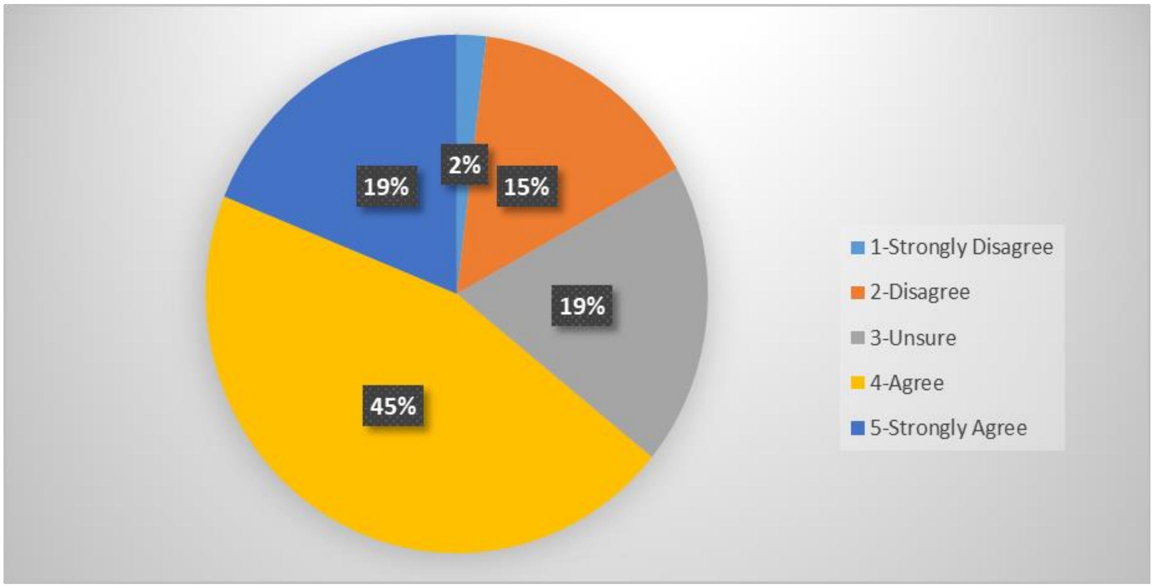


Figure 15: Implementing risk management strategies to mitigate potential risks.

Majority of respondents (45%) agreed that their team consistently implements risk management strategies to mitigate potential risks. Additionally, 19% of respondents strongly agreed with the statement. However, a notable percentage of respondents (15%) disagreed with the statement, and 19% expressed uncertainty about their team's consistency in implementing risk management strategies.

4.2.6 Research Question Six: On a scale of 1 to 5, where 1 is "Strongly Disagree" and 5 is "Strongly Agree" please rate the following statements regarding your team's assessment of risk management and prioritization of risk management activities:

Our team regularly reviews and updates our risk management plans to ensure they remain effective.

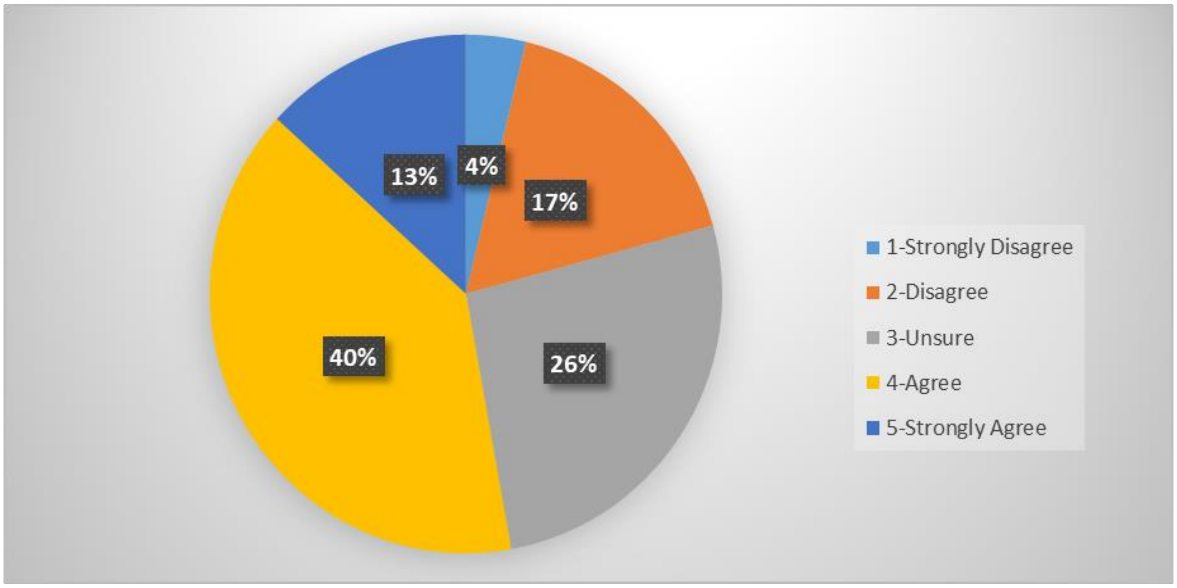


Figure 16: Regular review of risk management plans.

Majority of respondents (40%) agreed that their team regularly reviews and updates their risk management plans to ensure they remain effective. Additionally, 13% of respondents strongly agreed with the statement. However, a notable percentage of respondents (17%) disagreed with the statement, and 26% expressed uncertainty about their team's regularity in reviewing and updating risk management plans.

4.2.7 Research Question Seven: On a scale of 1 to 5, where 1 is "Strongly Disagree" and 5 is "Strongly Agree" please rate the following statements regarding your team's assessment of risk management and prioritization of risk management activities:

Our team learns from past experiences and incorporates those lessons into our risk management practices.

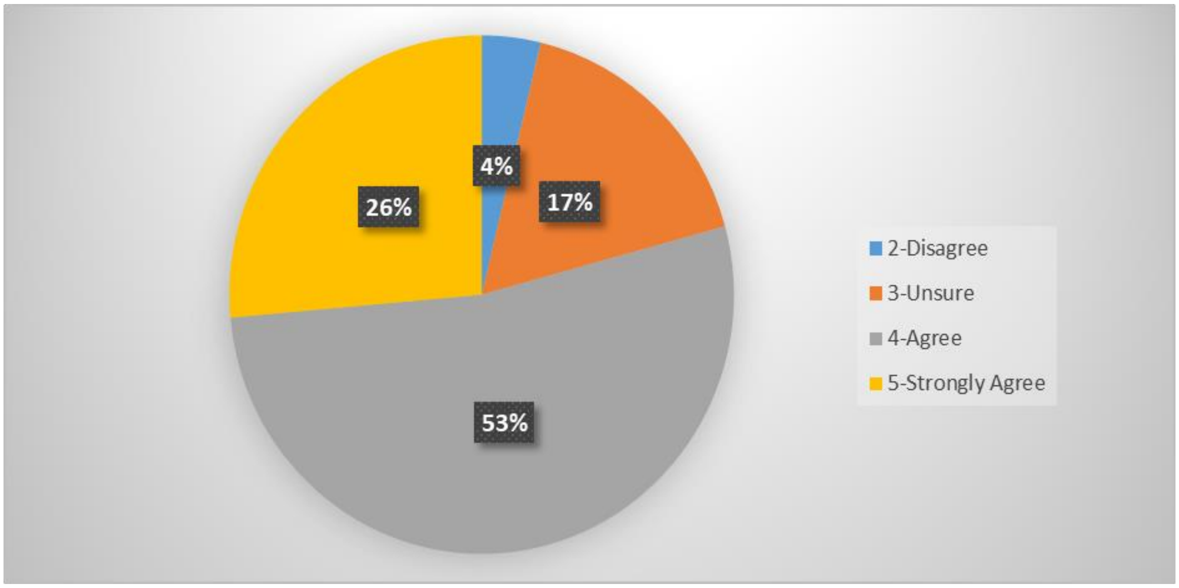


Figure 17: Incorporating lessons into risk management practices.

Majority of respondents (53%) agreed that their team learns from past experiences and incorporates those lessons into their risk management practices. Additionally, 26% of respondents strongly agreed with the statement. However, a small percentage of respondents (4%) disagreed with the statement, and 17% expressed uncertainty about their team's ability to learn from past experiences and integrate them into risk management practices.

4.2.8 Research Question Eight:

Select Top 5 common risks hampering your project?

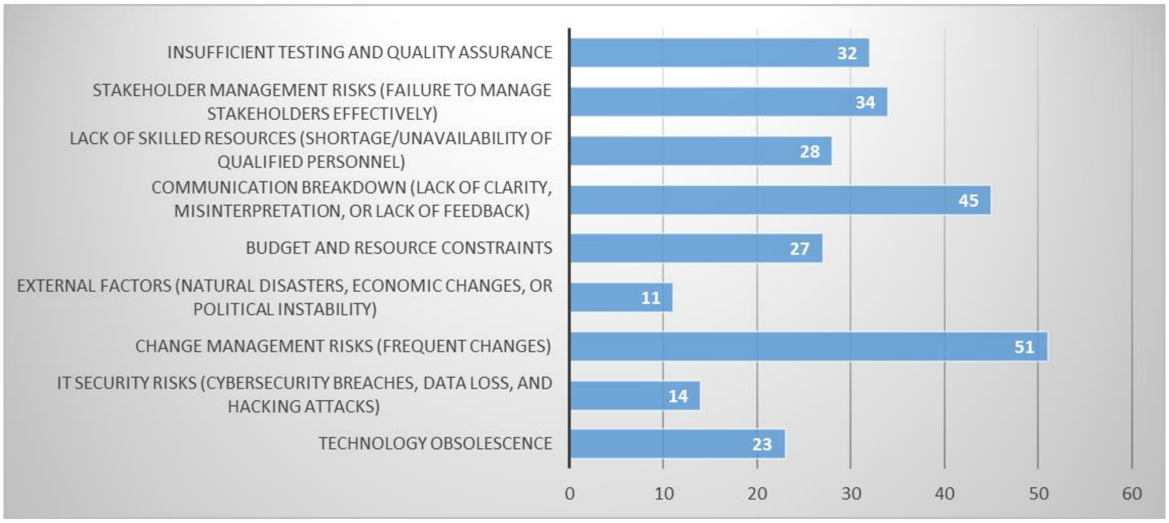


Figure 18: Common risks hampering project.

Top 5 common risks hampering projects in the IT industry are as follows:

1) Change management risks (Frequent Changes): 51
2) Communication breakdown (lack of clarity, misinterpretation, or lack of feedback): 45
3) Stakeholder management risks (Failure to manage stakeholders effectively): 34
4) Insufficient testing and quality assurance: 32
5) Budget and resource constraints: 27

4.2.9 Research Question Nine: On a Likert scale from 1 to 5, where 1 represents “Not Confident at all” and 5 represents "Very Confident"

How confident are you in your organization's ability to handle unexpected risks?

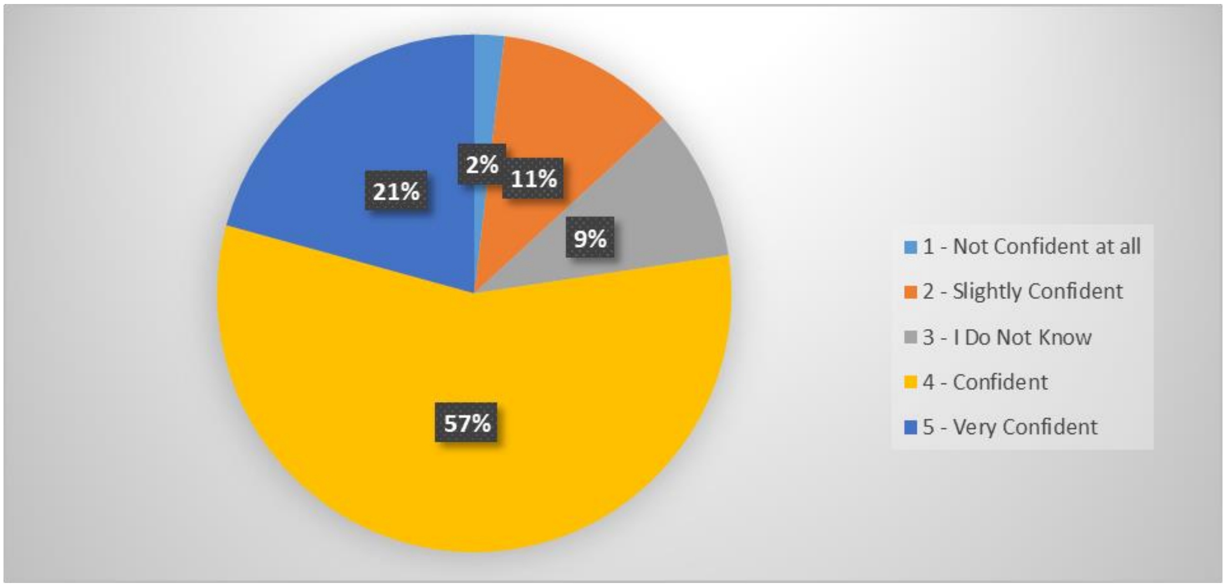


Figure 19: Organization's ability to handle unexpected risks.

Majority of respondents (57%) expressed confidence in their organization's ability to handle unexpected risks. Additionally, a notable percentage of respondents (21%) indicated being very confident in their organization's capabilities. However, a small percentage of respondents (2%) reported not being confident at all, and 9% expressed uncertainty regarding their organization's ability to handle unexpected risks.

4.2.10 Research Question Ten: On a Likert scale from 1 to 5, where 1 represents “Not Confident at all” and 5 represents "Very Confident"

How confident are you in your ability to handle unexpected risks?

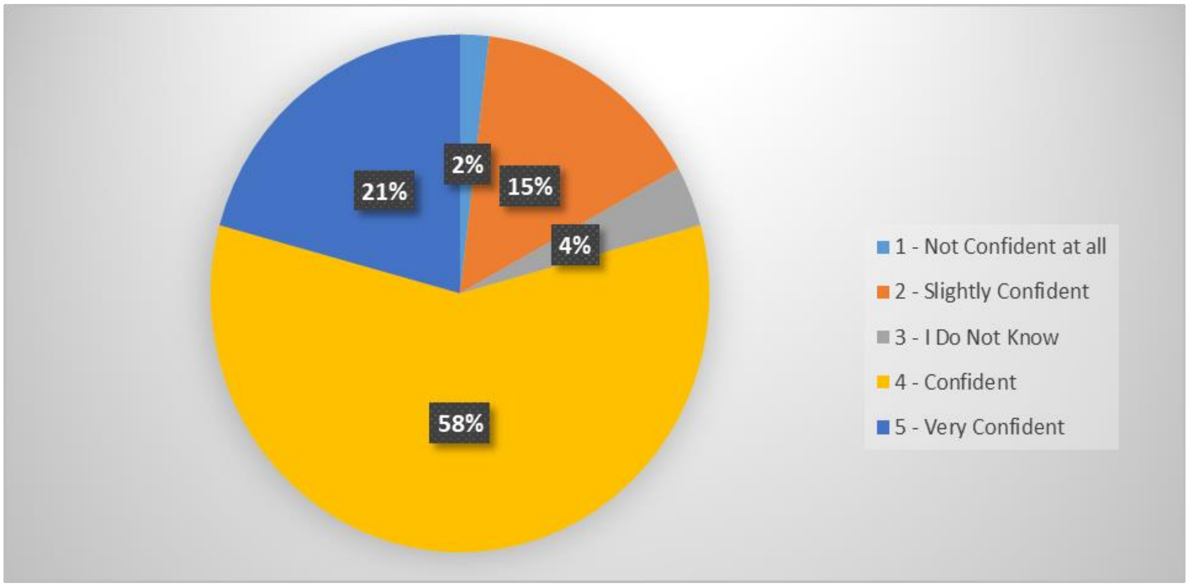


Figure 20: Individual’s ability to handle unexpected risks.

Majority of respondents (58%) expressed confidence in their ability to handle unexpected risks. Additionally, a notable percentage of respondents (21%) indicated being very confident in their abilities. However, a small percentage of respondents (2%) reported not being confident at all, and 4% expressed uncertainty regarding their ability to handle unexpected risks.

4.2.11 Research Question Eleven: On a Likert scale from 1 to 5, where 1 represents “Never” and 5 represents "Always"

Our Team currently uses Artificial Intelligence tools for detecting and managing risk.

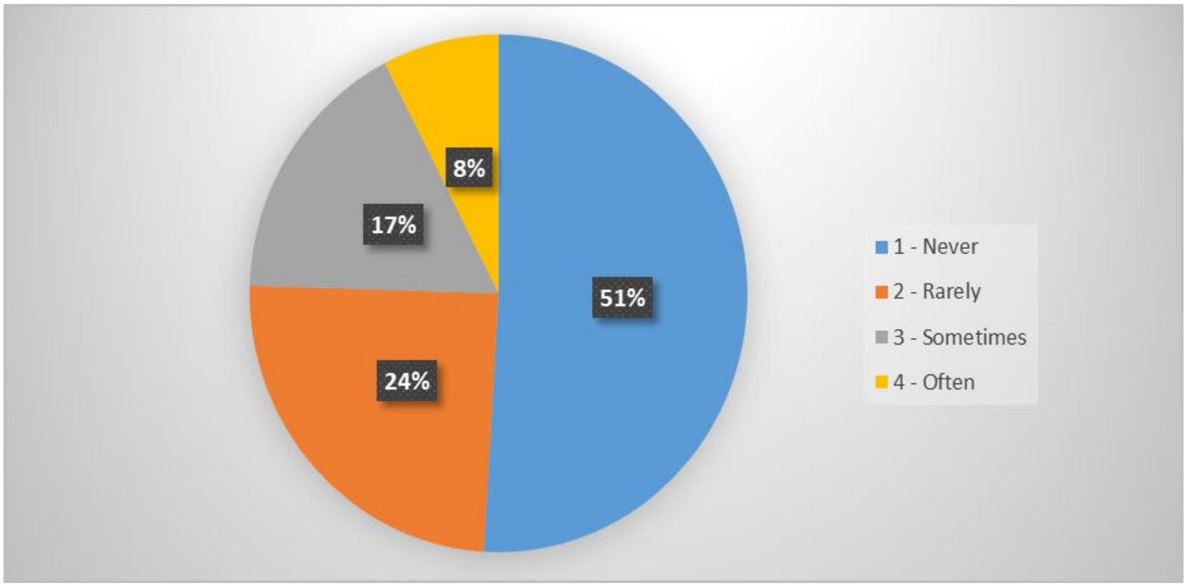


Figure 21: Using Artificial Intelligence tools for detecting and managing risk.

Majority of respondents (51%) reported that their team never uses Artificial Intelligence tools for detecting and managing risk. Additionally, 25% of respondents indicated that Artificial Intelligence tools are rarely used, while 17% mentioned that they are used sometimes. A small percentage of respondents (8%) reported that their team often uses Artificial Intelligence tools for this purpose.

4.3 Interview Result

4.3.1 Interview Question 1

1) Can you provide an overview of your experience with project management in the IT industry and your familiarity with risk assessment practices?	***Project Manager 1:*** I have been working within this field for more than 10 years now. I have experienced several external and internal events that have created challenges for the entire team. Throughout my career, I have gained extensive experience in project management within the IT industry. I have successfully managed various projects, ranging from software development to infrastructure implementation. In each project, I have recognized the importance of risk assessment and its impact on project outcomes. ***Project Manager 2:*** I am well-versed in conducting risk assessments as an integral part of project planning. I have utilized different techniques such as identifying potential risks, assessing their likelihood and impact, and developing appropriate risk mitigation strategies. I am familiar with qualitative and quantitative risk assessment approaches and have applied them to prioritize and manage risks effectively. ***Executive 1***: I understand the significance of continuous risk monitoring and have implemented processes to regularly review and update risk assessments throughout the project lifecycle. I believe in proactive risk management and take a proactive approach to identify and address potential risks before they escalate into significant issues.

	Executive 2: I have also collaborated with cross-functional teams and stakeholders to gather insights and perspectives on project risks. This collaborative approach ensures that risk assessment is comprehensive and considers diverse viewpoints. Overall, my experience in project management within the IT industry has allowed me to develop a strong understanding of risk assessment practices and their importance in delivering successful projects.

4.3.2 Interview Question 2 **2) Have you had any prior experience or exposure to using artificial intelligence tools for risk assessment in project management?**	***Project Manager 1:*** I don't have personal experience with using Artificial Intelligence tools and I am interested to explore if any tools are available and want to see how we can use it to assess project related risks. I definitely support using Artificial Intelligence tools in risk management & risk assessment. ***Project Manager 2:*** I understand Artificial intelligence tools are increasingly being used in project management to improve risk assessment and mitigation, but I have never used one in my current role. ***Executive 1***: Tools help project managers identify potential risks, assess their likelihood and impact, prioritize them, and develop effective risk mitigation strategies but I have personally not used one but would love to experience one. Machine Learning algorithms, natural language processing (NLP) techniques, analytical model and data visualization tools are something which are making lot of buzz in the industry and want to leverage the same for our business unit.

	Executive 2: I don't have personal experiences or direct exposure to using artificial intelligence tools for risk assessment in project management.

4.3.3 Interview Question 3 **3) How do you see the role of artificial intelligence tools in enhancing risk assessment and management in project management for the IT industry?**	***Project Manager 1:*** Artificial Intelligence tools can monitor project-related data and other factors to gain real-time insight into emerging risks. Using real-time data, project managers can identify trends, vulnerabilities or potential risks and respond quickly to minimize their impact. ***Project Manager 2:*** Artificial Intelligence tools, especially those combined with predictive analytics, can analyze historical data and external factors to predict future risks. By considering patterns and patterns, these tools predict the likelihood and impact of risks, allowing project managers to allocate necessary resources and plan strategy to mitigate risk first. ***Executive 1***: Artificial Intelligence tools can perform routine risk assessments, freeing managers to focus on higher-level decision making. This automation increases efficiency, reduces human error, and enables managers to allocate their time and expertise more strategically.

	Executive 2: Artificial Intelligence tools can process and analyze massive amounts of data from multiple sources, including operational data, historical data, business models, and external data. By analyzing this data, Artificial Intelligence tools can identify patterns, relationships, and risks that cannot be easily discovered with manual analysis. This enables us to make more informed decisions and take proactive steps to reduce risk.

4.3.4 Interview Question 4 **4) What challenges or limitations do you anticipate when using artificial intelligence tools for risk assessment in the IT industry?**	***Project Manager 1:*** Artificial Intelligence tools rely on good and relevant data for accurate risk assessment. However, data availability and performance can be challenging, especially in complex IT projects. Incomplete or inconsistent data can lead to inaccurate measurements and unreliable estimates. ***Project Manager 2:*** The IT industry is constantly evolving, and new technologies, threats and risks are constantly emerging. Artificial Intelligence tools can struggle to keep up with the current IT risk situation, requiring constant updates and upgrades to effectively address new and changing risks. ***Executive 1***: While Artificial Intelligence tools can replace some aspects of risk assessment, human intelligence and decision making are essential. Artificial Intelligence tools should be seen as decision support rather than human reasoning. It is important to strike a balance between the use of Artificial Intelligence capabilities and the integration of human insight and knowledge.

	Executive 2: Using Artificial Intelligence tools for risk assessment requires integration with existing project management processes and tools. Resistance to change, lack of organizational readiness, and the need to motivate employees can complicate the implementation and integration of Artificial Intelligence tools.

4.3.5 Interview Question 5 **5) How do you effectively communicate the results and recommendations derived from artificial intelligence tools to project stakeholders, including non-technical individuals?**	***Project Manager 1:*** A high-level explanation of how Artificial Intelligence tools work and specific applications. But avoid using technology. Additionally, communication limitations and uncertainties are associated with Artificial Intelligence models, including the potential for bias or areas that still require human judgment. This helps manage expectations and makes it easier to truly understand Artificial Intelligence -derived results. ***Project Manager 2:*** Use visual aids such as charts, graphs, and graphs to present the results from Artificial Intelligence in a visual and easy-to-understand way. Visual representations can help stakeholders quickly relate to data, recognize patterns, and understand the significance of findings. ***Executive 1***: Organize meetings, workshops, or presentations to engage stakeholders. Questions, discussions, and feedback are encouraged to facilitate two-way communication. Allow participants to share their thoughts, concerns, and insights, and to address any misunderstandings or uncertainties they may have about Artificial Intelligence outcomes.

	Executive 2: Tailor your communication to all stakeholders based on background, interests, and skill levels. Understand their specific needs and concerns and tailor messages accordingly. Customize content and presentation to ensure accuracy and clarity for all stakeholder groups.

4.4 Summary of Findings

Training in Risk Management: A significant proportion of respondents (15%) reported not receiving any training in risk management within their company. Most respondents (42%) had intermediate level training, while 23% had basic level training. A smaller percentage of respondents (19%) had advanced level training, and only 2% considered themselves experts in risk management.

Understanding of Risk Management: Most respondents (53%) believed that their team has a clear understanding of risk management principles and practices. However, a notable portion (21%) expressed uncertainty about their team's understanding, and 11% disagreed. On the positive side, 15% of respondents strongly agreed that their team has a clear understanding of risk management.

Effective Risk Assessment: A significant majority of respondents (66%) agreed that their team effectively assesses risks and identifies potential issues. A notable percentage (19%) strongly agreed, while a small percentage (2%) disagreed, and 13% were uncertain about their team's effectiveness in risk assessment.

Clear Process for Risk Prioritization: Most respondents (51%) agreed that their team has a clear process for prioritizing risk management activities. A smaller percentage (15%) strongly agreed, but a notable proportion (26%) expressed uncertainty about their team's clarity in prioritizing risks. Additionally, 8% disagreed with the statement.

Consistent Implementation of Risk Management Strategies: Most respondents (45%) agreed that their team consistently implements risk management strategies to mitigate potential risks. Furthermore, 19% of respondents strongly agreed. However, 15% disagreed with the statement, and 19% expressed uncertainty about their team's consistency in implementing risk management strategies.

Regular Review and Update of Risk Management Plans: Most respondents (40%) agreed that their team regularly reviews and updates their risk management plans to ensure they remain effective. Additionally, 13% strongly agreed. However, 17% disagreed, and 26% expressed uncertainty about their team's regularity in reviewing and updating risk management plans.

Learning from Past Experiences: Most respondents (53%) agreed that their team learns from past experiences and incorporates those lessons into their risk management practices. Furthermore, 26% strongly agreed. However, 4% disagreed, and 17% expressed uncertainty about their team's ability to learn from past experiences and integrate them into risk management practices.

Confidence in Handling Unexpected Risks: Most respondents (57%) expressed confidence in their organization's ability to handle unexpected risks, with 21% indicating being very confident. However, a small percentage (2%) reported not being confident at all, and 9% expressed uncertainty regarding their organization's ability to handle unexpected risks. Similarly, most respondents (58%) expressed confidence in their ability to handle unexpected risks, with 21% indicating being very confident. However, a small percentage (2%) reported not being confident at all, and 4% expressed uncertainty regarding their ability to handle unexpected risks.

Usage of Artificial Intelligence Tools: The data shows that a significant proportion of respondents (51%) reported that their team never uses Artificial Intelligence tools for detecting and managing risk. Furthermore, 25% mentioned that these tools are rarely used, 17% mentioned sometimes, and only 8% reported using them often.

Common Risks in the IT Industry: The top five common risks hampering projects in the IT industry, as reported by respondents, are change management risks (51%), communication breakdown (45%), stakeholder management risks (34%), insufficient testing and quality assurance (32%), and budget and resource constraints (27%).

These findings provide insights into the respondents' training levels, understanding of risk management, effectiveness in risk assessment and prioritization, implementation of risk management strategies, review, and update of risk management plans, learning from past experiences, confidence in handling unexpected risks, usage of Artificial Intelligence tools, and common risks in the IT industry. Organizations can use these findings to identify areas of improvement and strengthen their risk management practices accordingly.

4.5 Conclusion

In Conclusion, the document highlights several important aspects of risk management in the IT industry. Although the majority of respondents said they have never received any training in risk management, most have received secondary or basic training. This shows that there is a need for more and consistent training in the organization.

Committee responses to questions regarding the understanding of risk management and practices were generally positive, with the majority reported to have a clear understanding. However, there is a high degree of uncertainty and disagreement within the group, indicating the need for better communication and information transfer.

The risk assessment and performance analysis were rated positive, and the majority agreed that their team was effective in identifying risks and identifying potential issues. This demonstrates a solid foundation in risk management.

The majority reported having a clear upfront process for risk management, but many noted confusions in this area. Organizations should focus on establishing a clear and consistent process for prioritizing risk.

Most respondents reported that they followed risk management strategies and made efforts to reduce risks. However, a significant proportion disagree or misrepresent, pointing to the need for better coordination and effective risk management strategies.

Risk management plans are regularly reviewed and updated, and lessons learned from past experience are generally well appreciated. However, there are still participants who disagree or express uncertainty, emphasizing the importance of continuous improvement and knowledge sharing.

They are very confident in dealing with imminent danger, whether within the organization or at the individual level. This indicates a level of readiness and confidence in the team and organization's ability to respond to unforeseen challenges.

Reporting on the use of Artificial Intelligence tools for risk detection and management is limited, with a significant proportion of respondents reporting no or limited use. This provides organizations with an opportunity to explore the benefits of Artificial Intelligence tools in improving risk management.

Identify common IT business risks, including change management, networking, stakeholder management, poor testing and quality assurance, and financial and resource constraints, and provide insight into the challenges facing the group. Organizations should focus on addressing these risks to improve business performance and overall performance.

Overall, the findings highlight the importance of regular education, open communication, effective risk assessment and research into proactive, implementation strategies, risk management, continuous learning, and Artificial Intelligence tools in IT industry risk management practices. By addressing these areas, organizations can strengthen risk management and improve project outcomes.

CHAPTER V:

DISCUSSION

5.1 Discussion of Results

The survey results provide information on respondents' views and knowledge on risk management in the IT industry. This discussion will focus on documenting key concepts and highlighting their impact on organizations.

First, the survey showed that respondents (15%) indicated that their company did not receive training in risk management. This finding highlights the lack of knowledge and skills that organizations need to address. Providing a comprehensive and consistent approach can help employees understand and effectively manage risk.

The majority (53%) is correct when it comes to respondents' understanding of risk management and practices. This indicates a good foundation in risk management knowledge. However, it is worth noting that a significant portion of the respondents (21%) were not sure that their team understood the issue, and a small percentage (11%) did not agree with this statement. These results highlight the importance of developing an understanding of risk management and promoting effective communication within the team.

The results of risk assessment and analysis are generally positive, with the majority (66%) agreeing that their team is effective in assessing risk and analyzing potential issues.

This finding shows that organizations have developed effective risk assessment processes. However, a small percentage of respondents (2%) did not agree with this statement and stated that in some cases there may be room for improvement.

The survey also examined whether there were clear procedures for risk management beforehand. While the majority (51%) of respondents reported having a clear process, a significant number (26%) expressed their team's uncertainty about the fact that management is a priority in respecting risk, while a minority (8%) disagreed. This finding highlights the importance of developing a transparent and effective system in advance for risk monitoring to be effective.

When it comes to risk reduction, most respondents (45%) agreed that their team has implemented risk management strategies. This result demonstrates a commitment to reduce risks. But more importantly, most (15%) disagree with the statement that points to the need to improve and implement risk management strategies in organizations.

Regarding the continuous review and updating of the risk management process, most respondents (40%) agreed that their team is involved. This finding suggests an effective approach to risk management.

However, a significant proportion (17%) of respondents disagreed with this statement, and a large majority (26%) expressed uncertainty about whether their team had reviewed the project risk. This finding indicates that organizations should emphasize the importance of regularly evaluating and adjusting their risk management strategies to ensure their continued effectiveness.

The survey also explores what the team has learned from past experiences and how they have incorporated these lessons into risk management. Most respondents (53%) agree that their team demonstrates a commitment to continuous improvement by learning from past experience. However, a small minority (4%) did not agree with this statement, stating that there is a need for better information sharing and organizational practices.

Finally, the survey assesses the level of confidence respondents have in handling unexpected risks. Most say they are confident in their own abilities (58%) and their organization's capabilities (57%). This result demonstrates a level of preparedness and confidence in managing unforeseen challenges. However, it is important to mention the small percentage of respondents who express confidence or uncertainty as this may indicate potential for improvement in risk management.

Overall, the findings demonstrated many aspects of risk management in the IT industry, including education, understanding of principles and practices, assessing risk, prioritizing, mitigating, reviewing, and updating plans, learning from experience, and resolving trust issues. risk.

These findings provide organizations with valuable information on identifying areas for improvement and improving risk management, ultimately improving project success, and reducing project failures.

5.2 Discussion of Survey Research Questions

5.2.1 Discussion of Research Question One

The research question aimed to assess the level of training received by respondents in risk management within their companies. The results provide insights into the extent of training provided and the distribution of respondents across different levels of training.

Most of the respondents (42%) stated that they received moderate training in risk management. This shows that organizations recognize the importance of developing employees with risk management and skills. Secondary education can provide people with a better understanding of risk management principles and enable them to participate in risk assessment and mitigation processes.

Most respondents (23%) reported having basic training in risk management. Basic training means that the organization recognizes the need for some level of risk management, but there will still be room for more depth and understanding of the training offered.

On the other hand, a small proportion (19%) of respondents said they have advanced training in risk management. Advanced training demonstrates that an organization invests in developing the skills of its employees, enabling them to manage dangerous situations and make informed decisions. This demonstrates an impact on risk management and commitment to developing high quality resources in the organization.

Few respondents (2%) see themselves as risk experts. This suggests that although some individuals have a great deal of knowledge and experience in the field, their representation in the responding group is limited. Organizations will benefit from identifying and using their skills to improve risk management.

Overall, the survey results show a good level of risk management education, with most respondents reporting intermediate education. However, there is still room for improvement, particularly in terms of providing further education and developing individuals to become risk experts.

Organizations can use these insights to adjust risk management training programs, address training gaps, and foster a culture of continuous learning and improvement.

5.2.2 Discussion of Research Question Two

The survey question was designed to measure respondents' perceptions of their team's understanding of risk management and practices, and their level of agreement with this statement. The results provide insight into each assessment of risk management understanding within the group.

Analyzed results show that most respondents (53%) agreed that their team had a clear understanding of risk management policies and practices. This shows that many groups already have a solid foundation in risk management, allowing them to effectively address risks. It shows how well the team has developed an understanding of the key concepts and opportunities related to risk management.

A significant proportion of respondents (21%) expressed uncertainty about their team's understanding of risk management. This uncertainty can be caused by many factors, including the lack of extensive training, lack of communication or advice on risk management, or the need for further clarification on certain aspects of risk management. Organizations can address this ambiguity by providing additional training, facilitating knowledge sharing, or encouraging open communication within teams about risk management.

A small percentage of respondents (11%) disagreed, stating that their team did not have a clear understanding of risk management and practices. This finding suggests that these groups may lack awareness or coordination in their risk management approach.

It is important that organizations identify and address gaps by providing training programs, facilitating collaboration, and providing resources to improve management practices.

Additionally, 15% of respondents agreed that their team had a clear understanding of risk management. This indicates that these groups are more confident in their awareness of risk and their practices. These groups will be more effective in identifying, analyzing and mitigating the risks that lead to success and increase the success of the organization.

Overall, the findings highlight the importance of ensuring that working groups have a clear understanding of risk management and its practices.

Organizations should consider investing in comprehensive training programs that promote open communication and provide ongoing support to improve risk management. By doing this, the team can better identify and deal with potential risks and increase the profitability and performance of the organization.

5.2.3 Discussion of Research Question Three

The question was designed to explore the extent to which respondents agreed with the statement and their views on the effectiveness of their teams in assessing risks and identifying potential problems. The results provide information on the overall assessment of the risk assessment within the group.

Overwhelming respondents (66%) agreed that their teams were effective in assessing risk and identifying potential issues. This finding indicates that most teams have established procedures and good practices to assess risks and identify potential issues. These groups may have good processes that allow them to identify and deal with risks, thus contributing to the success of the project.

One percent (19%) of respondents agree that their team is effective in identifying risks and identifying potential problems. This indicates that these groups are more confident and satisfied with their risk assessment abilities. This group will have a good understanding of the various risks, use appropriate tools and methods, and have the expertise necessary to be effective and mitigate any problems that may occur.

However, it is worth noting that a small percentage of respondents (2%) disagreed with this statement, meaning their group did not assess risk and identify potential problems. This finding suggests that there may be difficulties or flaws in the risk assessment process among these groups.

Organizations should explore the reasons behind this difference and take steps to improve risk assessment, such as providing additional training, practicing risk management or promoting a culture of risk awareness and accountability.

Additionally, 13% of respondents are unsure of their team's effectiveness in assessing risks and identifying potential issues. This uncertainty can result from unclear roles and responsibilities of the team, poor communication, and feedback, or limited best practices in risk measurement. Organizations can address this uncertainty by encouraging information sharing, facilitating regular risk assessments, or training, and encouraging open dialogue about the risk affected.

Overall, the findings suggest that most research groups have developed a good risk assessment that allows them to identify and address potential problems.

However, organizations should also be mindful of the small percentage of respondents who disagree or express uncertainty as it shows areas for improvement. By investing in training, developing a culture of risk awareness, and providing the necessary resources, organizations can improve their teams' ability to assess risk and identify potential issues, thereby improving project results and overall risk management.

5.2.4 Discussion of Research Question Four

The survey question sought to understand respondents' perceptions of their team's ability to prioritize risk management and whether they believed their team had clear processes to do so. The results show the extent to which the participants agreed with this statement.

51% of respondents agree that their group has a clear upfront process for risk management. This suggests that most of the groups surveyed have developed methods or processes to prioritize risk management. These groups understand the importance of assessing and addressing risks according to their impact and probability, allowing them to allocate resources and monitor accordingly.

Most respondents (26%) were unsure of the fact that their group had a priority in risk management. This uncertainty can be caused by the lack of clear instructions, bad practices, or poor communication within the team. It suggests that there may be room for improvement in establishing more transparent processes and mechanisms for proactive risk management. Organizations should focus on clarifying and guiding groups in this area, making sure everyone understands what risks to take first and how to deal with them.

On the other hand, 15% of respondents agree that their group has a clear process for significant risk management work.

This shows that these groups have a clear and effective strategy while demonstrating their confidence and enthusiasm. These groups may view risk management as a priority and allocate resources and attention accordingly.

However, it is worth noting that 8% of respondents did not agree with this statement, indicating that their group does not have a clear process for important work in risk management hmm. This finding suggests that this group may have competition or disadvantage in pre-existing risk factors. Organizations should investigate the reasons behind this discrepancy and take steps to improve the accuracy and effectiveness of the risk management process.

As a result, while most respondents agree that their group has a clear process for risk management upfront, there is still room for improvement. Organizations should focus on providing clearer information, facilitating effective communication, and creating a way to manage risk proactively and effectively. By empowering teams to prioritize, organizations can allocate resources more efficiently and minimize the impact of unforeseen events.

5.2.5 Discussion of Research Question Five

The survey question was designed to measure respondents' perceptions of their teams using risk management strategies to mitigate risk. The results provide useful information about the level of agreement among stakeholders and the effectiveness of risk management within the surveyed team.

45% of respondents agree that their teams use risk management strategies to mitigate risks. This suggests that most groups consider it a good way to manage risk and use strategies to deal with risk. These groups will have established procedures and practices for identifying, analyzing, and mitigating risks, allowing them to minimize the adverse effects of never-before-seen uncertainties and events.

A significant proportion of respondents (19%) agree that their team implements risk management strategies. This indicates that there is trust and satisfaction among these groups and that they have risk management and practices. They prioritize reducing risk and making it an integral part of their operations or organizational processes.

However, it is worth noting that 15% of respondents disagree with this statement, indicating that they do not follow their group's risk management strategies. This finding suggests that there may be differences or deficiencies in the risk management of these groups that may increase their risks and outcomes.

Organizations should explore the reasons behind these differences and identify areas to improve their risk management approaches. Addressing these gaps is critical to ensure risks are adequately managed and mitigated.

Additionally, 19 percent of respondents are unsure of their social group when using risk management strategies. This uncertainty may be due to a lack of clarity or understanding of risk management within the team, or a lack of communication and training in this area. Organizations should focus on providing adequate training, guidance, and support to improve team understanding and the implementation of risk management strategies.

As a result, while most respondents agreed that their teams are pursuing risk management strategies, some teams still have room for improvement. Organizations should seek to establish a culture of risk awareness, provide appropriate training and resources, and establish effective risk management systems and make effective use of risk management strategies. By doing this, the team can better mitigate risks and protect project or organizational goals.

5.2.6 Discussion of Research Question Six

This survey question is designed to measure respondents' perceptions of their group's approach to reviewing and modifying risk management programs to ensure their effectiveness. The results provided useful information on the level of agreement among participants and suggested practices for the research group's risk management review and reform.

40% of respondents agreed that they regularly review and update their risk plans to ensure their teams are effective. This suggests that most research groups are involved in the process of reviewing and adjusting risk management. These groups recognize the importance of updating plans in a timely manner that allows them to adapt to changes and emerging risks.

Regular reviews and updates enable them to identify gaps or weaknesses in their risk management approach and implement appropriate improvements.

A significant proportion of respondents (13%) agree that their team is reviewing and updating their risk plans. This shows that these groups have developed good practices and have a good approach to risk management. They monitor the continuous development of risk management systems and are committed to improving their ability to identify, measure and respond to risks.

However, it is worth noting that many respondents disagreed or were unsure about the regularity of their teams reviewing and updating their risk plans.

17% of respondents disagree and 26% are unsure whether their team is following the rules. This finding points to differences or inconsistencies in group risk management. This indicates that some groups may not be adequately allocated or resourced to review and update processes, which can at times lead to ongoing risk management programs that are not adequately addressed.

To ensure the effectiveness of the risk management system, the organization should emphasize the importance of regular review and update. This can be done through training and awareness programs that provide clear guidelines and standards for evaluating projects and fostering a culture of continuous improvement.

By encouraging teams to regularly evaluate and adjust their risk management systems, organizations can improve their ability to identify and mitigate risks.

In summary, although most respondents acknowledged that their teams have reviewed and updated their risk plans, some teams still have room for improvement. Organizations should highlight the value of this practice, provide appropriate support and resources, and promote a culture of continuous improvement in risk management. By doing this, teams can ensure that risk management remains effective and adapt to the changes and challenges they face.

5.2.7 Discussion of Research Question Seven

The survey question was designed to measure participants' perceptions of their team's ability to learn from past experiences and incorporate these lessons into risk management practices. The results provide insight into the level of agreement among participants and what groups have used in the past to improve their approach to risk management.

The majority (53%) of respondents agree that their team has learned from past experience and incorporated these lessons into risk management. This shows that a significant portion of the research team is involved in a culture of learning and understanding the value of using the past to improve risk management. These groups recognize that analyzing past activities, events or vulnerabilities can provide valuable insights and help them identify risks and implement risk mitigation strategies.

Additionally, 26% of respondents agree that their team has learned from past experience. This indicates that these groups have well-established processes for collecting and documenting learning and are using these lessons to improve their risk management. Using information from previous projects or events, these groups can anticipate and mitigate risks and improve profitability and risk management.

However, it is worth noting that a small percentage of respondents (4%) disagree with this statement, suggesting that their group may not be the main focus of learning past lessons or working hard to apply these lessons effectively in their risk management practices. Additionally, 17 percent of respondents are unsure of their team's ability to learn from past experience.

This suggests that there may be room for improvement in the way these groups share information, draw lessons learned, and apply those lessons to risk management activities.

To improve the integration of lessons learned into risk management, the organization should foster a culture of continuous learning and knowledge sharing. This can be achieved through processes such as post-work reviews, regular team discussions, and documentation of best practices and lessons learned. Providing resources and training on knowledge management and ensuring effective communication within the team can facilitate knowledge transfer and support the risk management approach.

In conclusion, while most respondents agree that their teams have learned from experience and incorporated those lessons into risk management, some teams still need improvement.

Organizations must develop a culture of learning and develop processes to capture and use lessons learned effectively. By doing this, the team can use their collective knowledge to improve their approach to risk management and improve project outcomes.

5.2.8 Discussion of Research Question Eight

The survey aimed to identify the top five common risks that hamper projects in the IT industry. The responses provided insights into the key challenges that project teams face, which can impact project success and delivery. The following are the top five risks identified based on the survey results:

a) **Change management risks (Frequent Changes)**: A significant majority of respondents (51) identified change management risks as one of the top challenges they face. This indicates that frequent changes in project requirements, scope, or technology can introduce uncertainties and complexities, making it difficult to effectively manage and deliver projects on time and within budget. It highlights the importance of having robust change management processes in place to handle changes efficiently and minimize their impact on project outcomes.

b) **Communication breakdown (lack of clarity, misinterpretation, or lack of feedback):** Communication breakdown was reported by 45 of the respondents as a significant risk. Ineffective communication within the project team, with stakeholders, or across different teams can lead to misunderstandings, delays, and errors. Clear and open communication channels, regular feedback mechanisms, and ensuring a shared understanding of project goals and requirements are crucial for addressing this risk.

c) **Stakeholder management risks (Failure to manage stakeholders effectively):** 34 of the respondents highlighted stakeholder management risks as a common challenge. Inadequate stakeholder engagement and failure to address their expectations, needs, and concerns can lead to project delays, scope creep, and conflicts. Proactive stakeholder identification, communication, and involvement throughout the project lifecycle are essential for managing this risk and ensuring stakeholder satisfaction.

d) **Insufficient testing and quality assurance**: 32 of the respondents identified insufficient testing and quality assurance as a significant risk. Inadequate testing practices and quality assurance processes can result in the delivery of subpar or defective products or services, leading to customer dissatisfaction and project failures. Robust testing and quality assurance frameworks, including comprehensive test plans, test cases, and continuous monitoring, are essential for mitigating this risk and ensuring the delivery of high-quality outputs.

e) **Budget and resource constraints**: Budget and resource constraints were mentioned by 27 of the respondents as a common risk. Limited financial resources and inadequate availability of skilled personnel, equipment, or technology can hinder project execution and compromise project outcomes. Effective resource allocation, careful budget planning, and leveraging external expertise or partnerships can help mitigate this risk and ensure optimal utilization of available resources.

These findings highlight the multifaceted nature of project risks in the IT industry. Addressing these risks requires a comprehensive approach, including effective change management, communication strategies, stakeholder engagement, testing and quality assurance practices, and resource management. By proactively identifying and managing these risks, project teams can enhance their chances of successful project delivery and mitigate potential negative impacts on project objectives.

5.2.9 Discussion of Research Question Nine

This survey question is designed to measure respondents' confidence in their organization's ability to deal with unforeseen risks. The results provide insight into the level of confidence and assurance individuals have about their organization's ability to manage unforeseen challenges. Here is an in-depth discussion of the findings:

The majority of respondents (57%) expressed confidence in their organization's ability to deal with unexpected risks. This demonstrates the appropriate level of confidence in their organization's readiness and ability to deal with unforeseen events or situations. This indicates that they believe their organization has the appropriate strategies, resources, and processes to respond to and mitigate risks when they occur.

21% of respondents reported that they trust their organization's resources. These groups radiate confidence and belief in their organization's ability to handle unforeseen risks. Their strong beliefs show that they believe their organization is efficient, well-organized, and capable of handling difficult situations.

On the other hand, a small percentage of respondents (2%) expressed distrust in their organization's ability to deal with unforeseen risks. This indicates a lack of trust or the ability to manage their organization.

Individuals in this group may feel that their organization is not ready to respond effectively to unforeseen risks, leading to concerns about the overall resilience and capacity of the organization. Nature solves problems.

A significant proportion of respondents (9%) are unsure of their organization's ability to deal with unexpected risks. This uncertainty can be caused by many factors, including the organization's lack of knowledge or insight into risk management or a lack of clear communication about risk mitigation strategies. It demonstrates the need for greater transparency and communication from organizational leaders to promote trust and transparency in risk management.

Overall, survey results show mixed confidence in organizations' ability to deal with unexpected risks.

Most respondents expressed confidence while some expressed doubt or uncertainty. This demonstrates the importance of effective communication, transparent risk management and continued efforts to improve organizational strength. Organizations must work to solve problems, provide training and support, and develop a culture of risk management to provide confidence and preparedness for unexpected problems.

5.2.10 Discussion of Research Question Ten

The question was designed to measure respondents' confidence in their ability to deal with unexpected risks. The results provide insight into a person's ability to understand themselves and cope effectively with unforeseen challenges. Below is an in-depth discussion of the findings:

The majority of respondents (58%) expressed confidence in their ability to cope with unexpected risks. This indicates that these individuals believe in their ability to protect and respond to unforeseen events or situations. They may have the knowledge, skills and experience they believe will enable them to effectively manage emerging risks.

A significant portion of the participants (21%) stated that they were very confident in their abilities. This group displays strong self-confidence and a strong belief in their ability to deal with unexpected risks. Strong beliefs indicate that they believe they are well prepared, able to act effectively, and have the ability to respond to and mitigate risks.

On the other hand, a small percentage of respondents (2%) expressed distrust in their ability to cope with unexpected risks. This indicates a lack of self-confidence or a belief that they have insufficient risk management skills and knowledge.

Individuals in this group may feel excited or unable to cope well and minimize unforeseen risks, which can lead to increased risk-taking and stress in the face of unforeseen circumstances.

A significant proportion (15%) of respondents expressed uncertainty about their ability to cope with unexpected risks. This uncertainty can be caused by many factors, such as lack of experience or lack of confidence in one's ability to manage risk. Indicates that further development, training, or support is needed to improve an individual's ability to manage unexpected risks.

Overall, the findings show confidence in people's ability to cope with unexpected risks. Most respondents expressed confidence while some expressed doubt or uncertainty about their abilities. This highlights the importance of continuing professional development, training and support to build confidence in self-advocacy and risk management. By investing in the development of skills and knowledge, people can better develop themselves to reduce and respond to unexpected challenges in their jobs.

5.2.11 Discussion of Research Question Eleven

The survey question was designed to measure the use of artificial intelligence (AI) tools in the respondent group to identify and manage risks. The results provide insight into the extent to which the research team is using Artificial intelligence tools in risk management. Here is an in-depth discussion of the findings:

The majority (51%) of respondents said their teams have never used Artificial intelligence tools to diagnose and manage risk. This suggests that Artificial intelligence tools are not currently integrated into the risk management processes of these groups. Reasons for this may vary, including limited knowledge or understanding of Artificial intelligence tools, limited use, or choice of alternative risk management methods.

Many respondents (25%) said their teams rarely use Artificial intelligence tools. This suggests that Artificial intelligence tools can be found or used occasionally but are not the primary or preferred method of research and management in this group. In these cases, other methods or means are more effective.

A significant proportion of respondents (17%) stated that artificial intelligence tools are sometimes used for risk detection and management. This reflects the centrality of integration and the use of Artificial intelligence tools in this group's risk management.

Rare use of Artificial intelligence tools may indicate that they are used selectively or for certain types of risk, rather than being used consistently across all risk management processes.

A small percentage (8%) of respondents said their teams regularly use Artificial intelligence tools to detect and manage risk. This indicates greater integration and reliance on Artificial intelligence tools in risk management among these groups. The continued use of Artificial intelligence tools can offer effective methods for risk detection, analysis and mitigation, using the potential of Artificial intelligence to increase the efficiency and effectiveness of operational risk management.

Overall, the findings suggest that the use of Artificial intelligence tools to detect and manage risk is not common among research groups.

While most respondents indicated that they use little or no Artificial intelligence tools, there are groups that use Artificial intelligence tools in different ways, ranging from occasional to frequent use.

Low adoption of Artificial intelligence tools in risk management may be due to many factors, such as awareness of Artificial intelligence capabilities, concerns about data privacy and security, requiring specialized skills or resources, or preference for traditional risk management. A willingness to use Artificial intelligence tools for risk management will be required to address these issues by providing education, raising awareness, addressing data security concerns, and seeing the value and benefits of Artificial intelligence integration in relational risk management.

As Artificial intelligence evolves and demonstrates its potential to improve risk management, expect more groups to discover and use Artificial intelligence tools to identify and manage risk. The findings highlight the status of the use of Artificial intelligence tools in risk management and provide insight for organizations and teams looking to leverage Artificial intelligence capabilities in their management.

5.3 Discussion of Interview Research Questions

5.3.1 Discussion of Interview Question One

The interview questions were designed to assess respondents' experience and knowledge of project management in the IT industry, focusing on their knowledge and understanding of risk assessment. Below is a discussion of the responses provided by the respondents:

Project Manager 1 has Project management experience in the IT industry, having worked in the field for more than 10 years. They talked about the challenges arising from external and internal events and acknowledged the importance of risk assessment for the event. Although they did not provide specific details about the risk assessment information, their experience showed that they have a good understanding of risk management in IT projects.

Project Manager 2 demonstrates a good understanding of risk assessment.

They emphasize the use of a variety of techniques to identify and measure risk both qualitatively and quantitatively. Their knowledge of this process shows that they have a good understanding of the risk assessment in the planning process. They demonstrate effective risk management, emphasizing the development of risk reduction strategies.

Executive 1 recognizes the importance of continuous risk monitoring and highlights the need to review and update risk metrics throughout the lifecycle. Their focus on risk management demonstrates a proactive approach to identifying and addressing risks before they escalate.

While they did not provide specific examples, their emphasis on continuous monitoring and updating means a commitment to being vigilant and adapting to changing risk factors.

The 2nd executive introduced their collaborative approach to risk assessment, engaging with cross-functional teams and stakeholders to gather insights and perspectives. This collaborative approach provides a better understanding of risk and includes different perspectives that can improve the accuracy and effectiveness of risk assessment. Even if they do not understand the specific risk measures, their emphasis on collaboration demonstrates integrated and inclusive management of risk.

Overall, respondents' responses demonstrated a good understanding of risk assessment in IT business project management. They demonstrated their knowledge of various technologies, an effective approach to mitigation, continuous monitoring and collaboration with stakeholders.

5.3.2 Discussion of Interview Question Two

Interview question was designed to assess participants' experience or exposure to using artificial intelligence (AI) tools for risk assessment in project management. Below is a discussion of the responses by respondents:

Project Manager 1 expressed his curiosity and interest in using Artificial intelligence tools for assessment risk in project management. They acknowledged the benefits of using artificial intelligence in risk management and expressed their support for its use. Despite their lack of personal experience in using Artificial intelligence tools, their openness to explore and use new technologies demonstrates their positive attitude towards using new methods to assess risk.

Project Manager 2 is familiar with the use of Artificial intelligence tools in project management to improve risk assessment and mitigation. Although they have not used Artificial intelligence tools themselves in their current roles, their knowledge of Artificial intelligence tools' capabilities and their impact in risk assessment suggests they have some insight and understanding of the benefits of Artificial intelligence in this context.

The Executive 1 recognized the value of tools in risk assessment and expressed an interest in using artificial intelligence tools, particularly machine learning algorithms, language processing techniques (NLP), modeling and data visualization tools. Despite their lack of personal experience with Artificial intelligence tools, their knowledge of business trends, and their interest in integrating Artificial intelligence into enterprise risk management practices, they showed curiosity and willingness to explore new solutions.

The 2nd Executive stated that they have no personal knowledge or direct exposure to the use of artificial intelligence tools in project management for risk assessment. Although they did not provide further details, their responses showed that they were unfamiliar with artificial intelligence tools in this field.

Overall, respondents indicated different levels and knowledge on using AI tools for risk assessment in project management. Project Manager 1 and Executive 1 showed interest and openness in exploring and using artificial intelligence tools, while Project Manager 2 stated that they were aware of the consequences. On the other hand, Executive 2 does not have direct access to Artificial intelligence tools. It will be beneficial for the participants to develop their understanding and experience in this field to follow the technological process and develop their ability to influence the risk assessment chance in project management.

5.3.3 Discussion of Interview Question Three

The interview questions were designed to explore respondents' views on the role of artificial intelligence (AI) tools in improving risk management and governance in the IT industry. Below are the responses and discussions of the interviewees:

Project managers 1 describes the real-time monitoring capabilities of smart devices in terms of their ability to analyze project-related information and identify emerging risks in a timely manner. Using real-time insights, the project manager can prevent vulnerabilities and potential risks and reduce their impact on projects. These answers highlight the power and functionality that Artificial intelligence tools can bring to risk and management.

Project Manager 2 focuses on the predictive capabilities of Artificial intelligence tools, especially when combined with predictive analytics. They added that Artificial intelligence tools can analyze historical data and external events to predict future risks. These tools measure the likelihood and impact of risk by analyzing trends and patterns, allowing managers to effectively allocate resources and develop necessary risk mitigation strategies. These answers show the future of Artificial intelligence tools in risk assessment and management.

Executive 1 highlights the role of Artificial intelligence tools in routine risk assessment, freeing operational managers to focus on higher-level decision making. Automation enabled by Artificial intelligence tools increases efficiency and reduces human error, allowing managers to use their time and expertise. These responses highlight the effectiveness and potential of Artificial intelligence tools in improving risk management decision making.

Executive 2 said Artificial intelligence tools can analyze big data from a variety of sources, including operational data, historical data, business models, and external data. Artificial intelligence tools can make more informed decisions and reduce risk by uncovering patterns, relationships, and risks that are difficult to identify with manual analysis. These answers highlight the potential of Artificial intelligence tools to support data-driven insights for risk assessment and quality control.

Overall, respondents recognize the value of Artificial intelligence tools in improving risk management and governance in the IT industry. Their responses highlighted key areas such as real-time monitoring, predictive capabilities, automation and data analytics. Using Artificial intelligence tools, organizations can gain insights, predict risk, automate operations, and make informed decisions to reduce risk. Participants understand the potential of Artificial intelligence tools to improve traditional risk assessments and improve outcomes in the IT industry.

5.3.4 Discussion of Interview Question Four

Interview question explore the challenges or limitations that can arise when using artificial intelligence (AI) tools for risk assessment in the IT industry. Below is a discussion of the responses provided by the respondents:

Project Manager 1 mentioned issues with data availability and quality. Artificial Intelligence tools rely on accurate and relevant data for accurate risk assessment. However, obtaining complete and consistent information on complex IT projects can be difficult. Incomplete or inconsistent data can lead to inaccurate measurements and unreliable estimates.

These responses highlight the importance of good data and the potential challenges of obtaining appropriate data for Artificial Intelligence based risk assessment.

Project Manager 2 focuses on the positive nature of the IT industry. As technology evolves, new threats and risks are constantly emerging. Artificial Intelligence tools can struggle to keep up with these changing risks and must adapt and adapt to deal with new and changing risks. These answers highlight the need to continually evaluate and adapt Artificial Intelligence tools to ensure their relevance and effectiveness in a changing IT environment.

Executive 1 emphasized the importance of combining human intelligence and decision-making with artificial intelligence tools. While Artificial Intelligence tools may replace some aspects of risk assessment, human insight and expertise will be essential. The integration of Artificial Intelligence tools should be seen as a decision support rather than a complete replacement for human reasoning. Striking the right balance between Artificial Intelligence capabilities and human experience is critical to providing effective testing. These answers highlight the need for collaboration that harnesses the power of artificial intelligence and human intelligence.

Executive 2 focuses on the challenges of integrating Artificial Intelligence tools into existing management processes and tools. The need to prevent change, organize the organization, and motivate employees can hinder the success and integration of Artificial Intelligence tools for risk assessment. These responses highlight the importance of addressing institutional and cultural issues to ensure smooth implementation of Artificial Intelligence tools and maximize their effectiveness.

Overall, respondents acknowledged that there are some challenges and limitations when using Artificial Intelligence tools for risk assessment in the IT industry. These include data availability and efficiency, keeping pace with dynamic IT environments, the role of human intelligence, and integrating Artificial Intelligence tools into already existing processes.

Understanding and solving these issues is critical to the success and use of Artificial Intelligence tools in risk assessment, allowing organizations to tap into the potential of Artificial Intelligence while reducing limitations.

5.3.5 Discussion of Interview Question Five

Interview question is aimed at effectively communicating the benefits and recommendations of artificial intelligence (AI) to stakeholders involved in the project, including employees, not experts. Below is a discussion of the responses from the respondents:

Project manager 1 suggested a high-level explanation of how the Artificial intelligence tool works and its text, especially when no descriptive words are used. This approach helps non-process stakeholders understand the benefits of Artificial intelligence analytics without the distraction of technology. It is also important to address the limitations or uncertainties associated with Artificial intelligence models, such as biases or domains that still require human judgment. These responses highlight the need for transparency and clear communication to manage stakeholder expectations and facilitate clear understanding of Artificial intelligence driven outcomes.

Project Manager 2 emphasizes the use of visual aids such as charts, graphs, and diagrams to present Artificial intelligence results in a clear and easy to understand way. Visual agents can help stakeholders quickly identify trends and understand the significance of findings. These responses validate the power of visual communication to make complex information more accessible and involve non-process stakeholders.

Executive 1 Guide to holding meetings, workshops, or presentations to engage stakeholders in two-way communication. Encouraging questions, discussions, and feedback allow participants to share their thoughts, concerns, and insights about Artificial intelligence results. This approach leads to a deeper understanding of Artificial intelligence outcomes and provides an opportunity to resolve any misunderstandings or uncertainties that stakeholders may have. It encourages collaboration and collaboration for effective communication.

The Executive 2 stressed the importance of cross-referencing the backgrounds, interests, and skills of various stakeholder groups. Understanding the specific needs and concerns of stakeholders helps tailor messages and presentations to be accurate and clear. This approach recognizes that effective communication requires adapting content and presentation to suit different audiences, which leads to better understanding and engagement.

Overall, respondents provided a good understanding of how to communicate Artificial intelligence benefits and recommendations to project stakeholders, including non-technical ones. These discussions include the use of clear, non-verbal language, visual aids, interactive communication, and appropriate communication to meet the needs of stakeholders, support understanding and encourage good cooperation. Using these techniques, the project manager can bridge the gap between Artificial intelligence understanding and stakeholder understanding, facilitating decision making and collaboration.

CHAPTER VI:

SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS

6.1 Summary

Survey results and interview responses shed light on various aspects of risk management and the integration of artificial intelligence (AI) tools into project management. According to the survey results, the key points are:

Survey Results:

Training Risk Management: Most of the respondents stated that they received training in risk management with the highest percentage being "Moderate". This indicates the appropriate level of knowledge and understanding of the respondents.

Team's Assessment of Risk Management: Overall, the findings demonstrated a good understanding of group risk management assessment and prioritization of risk management. Most respondents agree that their teams have a clear understanding of risk management and practices, effective risk assessment and clear processes primarily for risk management risk, implement risk management strategies, and have learned from previous lessons to improve risk management.

Common Risks: The survey identified several risks that could impact IT industry. These include change management risks, communications disruptions, budget and resource constraints, lack of intellectual capital, and stakeholder management risks.

Interview Response:

Risk Assessment Experience: Participants demonstrated that they have experience and knowledge of risk assessment in project management. They emphasized the importance of risk assessment for project results and emphasized the use of various techniques such as identifying risks, assessing their probability and impact, and creating risk reduction strategies.

Use of Artificial Intelligence tools: While some respondents were keen to explore the use of Artificial Intelligence tools for risk assessment, others acknowledged limited personal use of these tools. However, they recognize the potential of Artificial Intelligence tools, including the ability to monitor data in real time, predict future risks, automate daily risk measurements, and process large amounts of information for informed decision making.

Role of AI tools in risk assessment: Participants highlighted the role of Artificial Intelligence tools in project management to improve risk assessment and management. They highlighted benefits such as real-time insight into emerging risks, predictive analytics for future risk assessment, increased operational efficiency through the power of technology, and the ability to process and analyze large volumes of data to make informed decisions.

Challenges and limitations of Artificial Intelligence tools: Participants acknowledged the challenges and limitations of using Artificial Intelligence tools for risk assessment. These include data availability and quality issues, the need to constantly adapt to changing risks, human intelligence and decision making, as well as the importance of Artificial Intelligence tools and the integration of Artificial Intelligence tools with existing management processes and tools.

Communication of Artificial Intelligence results: Participants provided strategies to effectively communicate Artificial Intelligence results and recommendations to stakeholders, particularly the non-implemented machine. Recommendations include the use of enhanced narratives, visual aids, interactive communication, and communication based on content and interests of stakeholders.

The results of the survey show that respondents are interested in exploring the use of artificial intelligence tools for risk assessment. Although many of the participants did not have personal experience with these tools, they expressed their support and curiosity for their potential in this field. This demonstrates a growing awareness of the value Artificial Intelligence can bring to risk management in the IT industry.

Interviews with project managers and leaders give us a deeper understanding of their experiences and views. Obviously, some have experience in risk assessment using a variety of techniques to identify, quantify and mitigate risks.

However, they have limited access to Artificial Intelligence tools specifically designed for risk assessment. However, they acknowledged the importance of artificial intelligence in project management and expressed an interest in exploring and using this technology in their business.

Observations and interviews were consistent with the extensive literature review on the subject. The document highlights the role of Artificial intelligence tools in improving risk assessment and management in project management in the IT industry. AI tools can use real-time data to identify emerging risks, allowing managers to respond quickly and effectively.

In addition, by analyzing historical data and using predictive analytics, these tools can provide better insight into future risks, assist with resource allocation and strategic planning.

Despite the advantages, problems and limitations were also identified. Evaluators and responders expressed concern about the availability and quality of relevant information and the need for constant updating and updating to keep pace with the evolving IT environment. Artificial Intelligence tools should complement, rather than replace, human intelligence because human judgment and decision-making are important in managing risk.

Effective communication becomes crucial when smart tools are used for risk assessment.

Visualization tools such as charts and graphs are recommended as an effective way to present information derived from both technical and non-technical technology and artificial intelligence to stakeholders. It is also recommended that you engage stakeholders through meetings and training to facilitate two-way communication and resolve any uncertainties or concerns.

Observations and interviews together reflected the IT industry's growth in Artificial Intelligence tools for risk assessment. Although some participants did not have direct experience, they recognized the potential benefits and expressed interest in exploring this tool further. The findings suggest that organizations in the IT industry should consider using Artificial Intelligence tools for risk assessment when solving problems with available data, continuous learning, and good communication.

By doing this, they strengthen risk management and improve project outcomes. Overall, the findings and interview responses highlighted the importance of risk management in project management and highlighted the benefits and challenges of integrating Artificial Intelligence tools in this context. The findings highlight the importance of clear communication and collaboration with stakeholders when using Artificial Intelligence tools for risk assessment, as well as the need for continuous training and improvement in risk management.

6.2 Implications

Research into the use of artificial intelligence (AI) for risk assessment in project management in the IT industry has several important implications. These interventions are based on research results, interviews, and extensive literature review on the topic.

Adoption of Artificial Intelligence tools: Research shows that professionals in the IT industry are increasingly interested in exploring and using Artificial Intelligence tools for risk assessment. What this finding means is that organizations should consider incorporating Artificial Intelligence tools into their risk management processes to improve their ability to identify, measure and mitigate risks.

Skill Development: As Artificial Intelligence tools become more common in risk assessment, professionals need to acquire the skills and knowledge necessary to apply and interpret the results associated with the creation of this tool. This study highlights the importance of training and development programs for project managers and other stakeholders in Artificial Intelligence processes and risk assessment processes.

Data Management: Observations and interviews have highlighted the importance of having and doing good data for proper evaluation of intelligence tools. Organizations must ensure they have appropriate data management, including data collection, storage, and analysis, to better understand and improve risk outcomes.

Integration with existing processes: Integrating Artificial Intelligence tools into existing management processes requires careful integration and optimization. Organizations need to evaluate their current operations and identify opportunities for integration with Artificial Intelligence tools. This will include updating existing systems, establishing clear roles and responsibilities, and providing the resources and support necessary for success.

Continuing Learning & Adoption: The dynamic nature of the IT industry requires continuous learning and adoption when using Artificial Intelligence tools for risk assessment. Organizations should adopt a culture of continuous improvement and innovation that encourages employees to stay abreast of the latest in Artificial Intelligence technology and risk management.

Ethical considerations: This study highlights the need to address ethical issues related to data integrity, algorithmic transparency, and accountability. Organizations need to establish ethics and procedures to ensure responsible and fair use of Artificial Intelligence tools in risk assessment.

Effective communication: Observations and interviews have demonstrated the importance of effective communication when presenting Artificial Intelligence results and recommendations to stakeholders, including non-tech. Organizations should invest in improving communication and use visual aids to present complex information in a clear and understandable way.

Overall, research shows that the use of Artificial Intelligence tools for risk assessment in project management has the potential to improve risk management in the IT industry. However, special attention should be paid to solving problems related to knowledge, skills, coordination, ethics, and communication to obtain the best results and ensure the success of Artificial Intelligence tools in the risk assessment process.

6.3 Recommendations for Future Research

Based on the findings of surveys and interviews regarding the risks of using Artificial intelligence (AI) in project management in the IT industry, the following recommendations are offered. Volunteer research:

Longitudinal study: Conduct longitudinal studies to examine the long-term effects and outcomes of using Artificial intelligence tools for risk assessment in project management. This will provide a deeper understanding of how the adoption of Artificial intelligence tools evolves over time and its impact on project success.

Comparative Studies: Conduct comparative studies comparing the effectiveness of different intelligence tools and techniques in risk assessment. This will help identify the best Artificial intelligence tools for the environment and gain insight into their strengths and limitations.

Case Studies: Conduct in-depth case studies exploring the use of Artificial intelligence tools in risk assessment. These case studies provide insight into the challenges, benefits, and best practices associated with implementing Artificial intelligence tools across different industries and types of projects.

Fairness in decision making: More research is needed to determine fairness in decision making associated with the use of Artificial intelligence tools for risk assessment. This includes investigating vulnerabilities in Artificial intelligence algorithms, addressing algorithmic transparency and accountability issues, and exploring ethical decision making in Artificial intelligence driven risk assessment.

User Experience and Acceptance: Investigate the user experience and acceptance of Artificial intelligence tools for risk assessment among project managers and other stakeholders. These studies can help identify barriers to adoption, factors affecting user acceptance, and strategies to facilitate the effective use of artificial intelligence tools in the risk assessment process.

Integration with project management: Explore integrating Artificial intelligence tools for risk assessment with other project management systems and processes, such as agile or waterfall. Discover how Artificial intelligence tools can be integrated into existing systems and processes to increase the effectiveness of risk management.

Industry-specific Studies: Conduct industry-specific studies to understand the unique challenges and opportunities in using AI tools for risk assessment across different sectors within the IT industry. This can provide tailored insights and recommendations for specific industry contexts, such as software development, cybersecurity, or infrastructure projects.

Organizational Processes: Investigate organizations that influence the application and use of intelligence tools for risk assessment. This includes examining factors such as leadership, leadership support, resource allocation, and change management strategies.

Collaboration and Knowledge Sharing: Facilitating collaboration and knowledge sharing among researchers, practitioners, and industry professionals to develop a deeper understanding of intelligence tools for risk assessment. This can be done through conferences, workshops and seminars that facilitate the exchange of ideas, experiences, and best practices.

By addressing these research recommendations, future studies can contribute to the advancement of knowledge and practice in utilizing AI tools for risk assessment in project management within the IT industry.

6.4 Conclusion

In conclusion, this research paper focuses on research into the use of artificial intelligence (AI) tools for risk assessment in project management in the IT industry. This study brings together survey results, interviews and data analysis to understand current practices, perceptions and issues with the use of truly intelligent technology for risk assessment.

The survey results provided valuable insight into the extent to which respondents agreed or disagreed with various statements regarding risk management and the use of artificial intelligence. The interviews presented insights from project managers and executives, demonstrating their experience, knowledge of artificial intelligence tools, and their understanding of their role in enhancing risk assessment and management.

Based on the findings of the study, it can be concluded that artificial intelligence tools have the ability to improve risk assessment in project management in the IT industry.

Research results show that people prefer to use artificial intelligence tools for risk assessment and often express confidence in their ability to deal with unexpected risks. Participants highlighted the advantages of artificial intelligence tools in real-time monitoring, predictive analytics, automation, and data processing capabilities.

However, the study also revealed some issues and limitations in using artificial intelligence tools for risk assessment. These include issues with data availability and quality, the need for continuous updates to address emerging risks, the importance of human decision-making as artificial intelligence tools gain, and the integration of artificial intelligence tools into existing management processes. The implications of the study highlight the need for continued research and exploration in this area.

Recommendations for future research highlight the importance of longitudinal studies, comparative studies, case studies, ethical concerns, user experience, integration with project management, integration with project management practices, industry-specific investigations, organizational factors, and collaboration among researchers and practitioners.

Overall, this research paper contributes to the growing body of knowledge on using Artificial Intelligence tools for risk assessment in project management within the IT industry. It provides insights into the current perceptions and practices surrounding Artificial Intelligence tools and highlights the potential benefits and challenges associated with their adoption. By addressing the research recommendations, future studies can further enhance our understanding and promote the effective utilization of Artificial Intelligence tools for risk assessment, ultimately improving project management outcomes in the IT industry.

APPENDIX A

SURVEY COVER LETTER

Hello,

I hope this email finds you well. I am writing to invite you to participate in a research study that I am conducting on risk management practices in project management as part of my research program.

The purpose of this study is to gather information related to risks in project management, and I believe that your professional experience would provide valuable insights into this topic. Your participation in this study would be greatly appreciated. The survey will take approximately 4 minutes to complete, and your participation is entirely voluntary. You are free to withdraw at any time, and your responses will be kept completely confidential. Only the research team will have access to them. Your participation in this study will help us better understand risk management practices and contribute to the advancement of knowledge in this area.

If you are willing to participate, please click on the following link to access the survey: https://forms.office.com/r/MZCRYsb5nz

If you have any questions or concerns about this study, please do not hesitate to contact me. Your feedback is essential to the success of this research, and I am grateful for your time and effort in completing the survey.

Thank you for considering this invitation to participate in our study. Your contribution is highly valued.

APPENDIX B

INFORMED CONSENT

You are free to withdraw at any time, and your responses will be kept completely confidential. Only the research team will have access to them.

APPENDIX C

SURVEY QUESTIONS

1.On a Likert scale from 1 to 5, where 1 represents "None" 2 (Basic) 3 (Intermediate) 4 (Advanced) and 5 represents "Expert"

Please, rate the level of your received training in risk management in your company.Required to answer.

1- None

2 - Basic

3 - Intermediate

4 - Advanced

5 - Expert

2.On a scale of 1 to 5, where 1 is "Strongly Disagree" and 5 is "Strongly Agree" please rate the following statements regarding your team's assessment of risk management and prioritization of risk management activities.

Our team has a clear understanding of risk management principles and practices

1-Strongly Disagree

2-Disagree

3-Unsure

4-Agree

5-Strongly Agree

3.On a scale of 1 to 5, where 1 is "Strongly Disagree" and 5 is "Strongly Agree" please rate the following statements regarding your team's assessment of risk management and prioritization of risk management activities.

Our team effectively assesses risks and identifies potential issues

1-Strongly Disagree

2-Disagree

3-Unsure

4-Agree

5-Strongly Agree

4.On a scale of 1 to 5, where 1 is "Strongly Disagree" and 5 is "Strongly Agree" please rate the following statements regarding your team's assessment of risk management and prioritization of risk management activities.

Our team has a clear process for prioritizing risk management activities

1-Strongly Disagree

2-Disagree

3-Unsure

4-Agree

5-Strongly Agree

5.On a scale of 1 to 5, where 1 is "Strongly Disagree" and 5 is "Strongly Agree" please rate the following statements regarding your team's assessment of risk management and prioritization of risk management activities.

Our team consistently implements risk management strategies to mitigate potential risks

1-Strongly Disagree

2-Disagree

3-Unsure

4-Agree

5-Strongly Agree

6.On a scale of 1 to 5, where 1 is "Strongly Disagree" and 5 is "Strongly Agree" please rate the following statements regarding your team's assessment of risk management and prioritization of risk management activities.

Our team regularly reviews and updates our risk management plans to ensure they remain effective

1-Strongly Disagree

2-Disagree

3-Unsure

4-Agree

5-Strongly Agree

7.On a scale of 1 to 5, where 1 is "Strongly Disagree" and 5 is "Strongly Agree" please rate the following statements regarding your team's assessment of risk management and prioritization of risk management activities.

Our team learns from past experiences and incorporates those lessons into our risk management practices

1-Strongly Disagree

2-Disagree

3-Unsure

4-Agree

5-Strongly Agree

8.Select Top 5 common risks hampering your project?

A. Technology obsolescence
B. IT Security risks (Cybersecurity breaches, data loss, and hacking attacks)
C. Change management risks (Frequent Changes)
D. External Factors (natural disasters, economic changes, or political instability)
E. Budget and resource constraints
F. Communication breakdown (lack of clarity, misinterpretation, or lack of feedback)
G. Lack of skilled resources (shortage/unavailability of qualified personnel)
H. Stakeholder management risks (Failure to manage stakeholders effectively)
I. Insufficient testing and quality assurance

9.On a Likert scale from 1 to 5, where 1 represents “Not Confident at all” and 5 represents "Very Confident"

How confident are you in your organization's ability to handle unexpected risks?

1 - Not Confident at all

2 - Slightly Confident

3 - I Do Not Know

4 - Confident

5 - Very Confident

10.On a Likert scale from 1 to 5, where 1 represents “Not Confident at all” and 5 represents "Very Confident"

How confident are you in your ability to handle unexpected risks?

1 - Not Confident at all

2 - Slightly Confident

3 - I Do Not Know

4 - Confident

5 - Very Confident

11.On a Likert scale from 1 to 5, where 1 represents “Never” and 5 represents "Always"

Our Team currently uses Artificial Intelligence tools for detecting and managing risk

1 - Never

2 - Rarely

3 - Sometimes

4 - Often

5 - Always

APPENDIX D

INTERVIEW QUESTIONS

1) Can you provide an overview of your experience with project management in the IT industry and your familiarity with risk assessment practices?

2) Have you had any prior experience or exposure to using artificial intelligence tools for risk assessment in project management?

3) How do you see the role of artificial intelligence tools in enhancing risk assessment and management in project management for the IT industry?

4) What challenges or limitations do you anticipate when using artificial intelligence tools for risk assessment in the IT industry?

5) How do you effectively communicate the results and recommendations derived from artificial intelligence tools to project stakeholders, including non-technical individuals?

REFERENCES

Applegate, L.M., Austin, R.D. and Soule, D.L. (2009). *Corporate information strategy and management : text and cases*. Boston: Mcgraw-Hill Irwin.

Baccarini, D., Salm, G. and Love, P.E.D. (2004). Management of risks in information technology projects. *Industrial Management & Data Systems*, 104(4), pp.286–295. doi:10.1108/02635570410530702.

Bannerman, P.L. (2008). Risk and risk management in software projects: A reassessment. *Journal of Systems and Softwar*e, 81(12), pp.2118–2133. doi:10.1016/j.jss.2008.03.059.

Benko, C. and F Warren Mcfarlan (2003). *Connecting the dots: aligning projects with objectives in unpredictable times*. Boston: Harvard Business School Press.

Boehm, B. and Turner, R. (2003). Using risk to balance agile and plan- driven methods. *Computer*, 36(6), pp.57–66. doi:10.1109/mc.2003.1204376.

Boeing (1935). *Boeing: Checklists to Enhance Safety*. [online] Available at:https://www.boeing.com/features/innovation-quarterly/dec2016/feature-technology-checklist.page.

Bronte-Stewart, M. (2005). Developing a risk estimation model from IT project failure research'. School of computing, University of Paisley PA1 2BE. *Computing and information systems,* V9, n3, p.8-31

Brown, L. (2020). *What is Risk Management in Project Management*? [online] Invensys Learning Blog. Available at: https://www.invensislearning.com/blog/risk-management-in-project-management/

Carufel, R. (2019). *81 percent of risk management pros already seeing value of AI*. [online] Agility PR Solutions. Available at: https://www.agilitypr.com/pr-news/public-relations/81-percent-of-risk-management-pros-already-seeing-value-of-ai/.

Chatterjee, D. and Ramesh, V.C. (n.d.). Real options for risk management in information technology projects. *Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences. 1999. HICSS-32. Abstracts and CD-ROM of Full Papers*.

Chulkov, D.V. and Desai, M.S. (2005). Information technology project failures. *Information Management & Computer Security*, 13(2), pp.135–143. doi:10.1108/09685220510589316.

Department of Defense (2019). *DoD Digital Modernization Strategy*.

Dorfman, M.S. (2013). *Introduction to risk management and insurance*. Boston: Pearson.

Du, S., Keil, M., Mathiassen, L., Shen, Y. and Tiwana, A. (2007). Attention-shaping tools, expertise, and perceived control in IT project risk assessment. *Decision Support Systems*, 43(1), pp.269–283. doi: 10.1016/j.dss.2006.10.002.

Elkington, P. and Smallman, C. (2002). Managing project risks: a case study from the utilities sector. *International Journal of Project Management*, 20(1), pp.49–57. doi:10.1016/s0263-7863(00)00034-x.

Frohnhoefer, R.W. (2019). *Risk Assessment Framework.*

Gertz, R. (2022). *Risk management for projects*. [online] louderthanten.com. Available at: https://louderthanten.com/resources/risk-management/project-risk-analysis [Accessed 28 Feb. 2023].

Gilbert, N. (2019). *Project management software constantly evolves with the emerging technologies and approaches to planning, budg.* [online] Financesonline.com. Available at: https://financesonline.com/35-essential-project-management-statistics-analysis-of-trends-data-and-market-share/.

Hall, P. (2003). 'Killing IT Projects'. *Cutter IT Journal, the Journal of Information Technology Management* ©2003 Cutter Information LLC. Vol. 16, No. 12

Hinde, S. (2005). Why do so many major IT projects fail? *Computer Fraud & Security*, 2005(1), pp.15–17. doi:10.1016/s1361-3723(05)00148-x.

Jordan, E. and Silcock, L. (2005). *Beating IT risks*. Chichester J. Wiley..

Kaoru Ishikawa (1988). *Guide to quality control*. New York: Unipub/Quality Resources.

LaPrad, L. (2020). *Understanding Different Types of Risk in Project Management*. [online] teamgantt.com. Available at: https://www.teamgantt.com/blog/types-of-project-management-risk [Accessed 28 Feb. 2023].

Lessard, D.R. and Miller, R. (2001). Understanding and Managing Risks in Large Engineering Projects. *SSRN Electronic Journal*. doi:10.2139/ssrn.289260.

Mahaney, R.C. and Lederer, A.L. (2003). Information systems project management: an agency theory interpretation. *Journal of Systems and Software*, 68(1), pp.1–9. doi:10.1016/s0164-1212(02)00132-2.

Mind Tools (1996). *Brainstorming - Creativity Techniques from MindTools.com*. [online]Mindtools.com.Availableat:https://www.mindtools.com/brainstm.html.

Murthi, S. (2002). Preventive risk management software for software projects. *IT Professional,* 4(5), pp.9–15. doi:10.1109/mitp.2002.1041172.

Neill, T. and Leaney, J. (2001). Risk management for an open CBS project. *Proceedings. Eighth Annual IEEE International Conference and Workshop On the Engineering of Computer Based Systems-ECBS 2001*. doi:10.1109/ecbs.2001.922404.

Pennock, M.J. and Haimes, Y.Y. (2002). Principles and guidelines for project risk management. *Systems Engineering*, 5(2), pp.89–108. doi:10.1002/sys.10009.

Piney, C. (2003). *Risk identification: combining the tools to deliver the goods*. Paper presented at PMI® Global Congress 2003—EMEA, The Hague, South Holland, The Netherlands. Newtown Square, PA: Project Management Institute.

ProProfs Project Blog. (2017). *Why Do Projects Fail? | Common Reasons for Project Failure*. [online] Available at: https://www.proprofsproject.com/blog/common-reasons-for-project-failure/.

Ray, S. (2021). *The Risk Management Process in Project Management.* [online] ProjectManager.com. Available at: https://www.projectmanager.com/blog/risk-management- process-steps.

Reel, J.S. (1999). Critical success factors in software projects. *IEEE Software*, 16(3), pp.18–23. doi:10.1109/52.765782.

Remenyi, D. (1999). *Stop IT project failure through risk management.* Oxford: Butterworth Heinemann.

Samad, J. and Ikram, N. (2006). Managing the Risks: An Evaluation of Risk Management Processes. 2006 *IEEE International Multitopic Conference*. doi:10.1109/inmic.2006.358178.

Staff, I.A. (2016). *3 Premium Ways To Prevent IT Project Failure.* [online] Industry Analysts, Inc. Available at: https://www.industryanalysts.com/11616_y-soft/ [Accessed 1 Jun. 2023].

Taylor, J. (2004). *Managing Information Technology Projects*. New York: American Management Association.

Tiwana, A. and Keil, M. (2004). The one-minute risk assessment tool. *Communications of the ACM*, 47(11), pp.73–77. doi:10.1145/1029496.1029497.

Wallace, L. and Keil, M. (2004). Software project risks and their effect on outcomes. *Communications of the ACM*, 47(4), pp.68–73. doi:10.1145/975817.975819.

Wanner, R. (2015). *Project risk management: the most important methods and tools for successful projects*. Lexington, Us: Pm-Risk, . © By Roland Wanner.

Washington, T. (2020). *PPM 101 - Portfolio Risk Management.* [online] Acuity PPM. Available at: https://acuityppm.com/ppm-101-portfolio-risk-management/.

Whittaker, B. (1999). What went wrong? Unsuccessful information technology projects. *Information Management & Computer Security*, 7(1), pp.23–30. doi:10.1108/09685229910255

Wiegers, K. (1998.). *Know Your Enemy: Software Risk Management.* [online] Available at: http://www.pedrosoconsultoria.com.br/waUpload/know-your-enemy00121012015184500.pdf