VILNIAUS UNIVERSITETO
VERSLO MOKYKLA

INTERNATIONAL PROJECT MANAGEMENT PROGRAMME

Emilija Leonovaitė

THE FINAL MASTER'S THESIS

PROJEKTŲ PORTFELIO RIZIKŲ VALDYMO TOBULINIMAS TARPTAUTINĖJE DRAUDIMO BENDROVĖJE	**ENHANCING PROJECT PORTFOLIO RISK MANAGEMENT AT AN INTERNATIONAL INSURANCE COMPANY**

Student _____

(signature)

Supervisor_____

(signature)

Vytautas Pugačevskis,
Partn. Assoc. Prof.

Vilnius, 2024

TABLE OF CONTENTS

SANTRAUKA

VILNIAUS UNIVERSITETO VERSLO MOKYKLA

TARPTAUTINĖS PROJEKTŲ VADYBOS PROGRAMA

EMILIJA LEONOVAITĖ

PROJEKTŲ PORTFELIO RIZIKŲ VALDYMO TOBULINIMAS TARPTAUTINĖJE DRAUDIMO BENDROVĖJE

Magistro darbo vadovas – Vytautas Pugačevskis, Partn. Doc.

Darbas parengtas Vilniuje, 2024 m.

Darbo apimtis – 79 puslapiai.

Lentelių skaičius darbe – 8 vnt.

Paveikslų skaičius darbe – 4 vnt.

Literatūros ir šaltinių skaičius – 46 vnt.

Trumpas apibūdinimas: projektų portfelio rizikos valdymo branda atskleidžia įmonės gebėjimą nuosekliai panaudoti rizikos valdymo procesus strateginiams tikslams pasiekti. Norint pasiekti didesnę projektų portfelio rizikos valdymo brandą, reikia išsirinkti rizikų valdymo modelį, padedantį organizacijai įvertinti save pagal pripažintus standartus, taip nustatant pagrindą tobulėjimui, prisiderinant prie unikalių organizacijos poreikių. Vis dėlto, esamoje literatūroje vis dar trūksta išsamių tyrimų ir praktinių gairių, specialiai pritaikytų projektų portfelio rizikų valdymui, daugiausia dėmesio skiriant rizikų valdymui atskiruose projektuose.

Tikslas: įvertinti esamą tarptautinės draudimo bendrovės projektų portfelio rizikos valdymo brandą, nustatant spragas, bei sukurti rekomendacijų sąrašą projektų portfelio rizikų valdymo tobulinimui, atsižvelgiant į visos organizacijos ir projektų portfelio komponentų rizikos valdymo sistemos kontekstą.

Uždaviniai:

- **Atlikti išsamią literatūros apžvalgą** apie rizikos valdymo praktikas projektų portfeliuose, apimant platesnį įmonės ir projektų portfelio komponentų rizikos valdymo sistemos kontekstą.

● **Apžvelgti esamus rizikos valdymo standartus** ir parinkti tinkamiausią tyrimui, kartu **parenkant** ir tinkamą **rizikų valdymo brandos vertinimo modelį**.

● **Įvertinti esamą projektų portfelio rizikos valdymo brandos** lygį tarptautinėje draudimo bendrovėje, **nustatant spragas**, atsižvelgiant į visos organizacijos ir projektų portfelio komponentų rizikos valdymo sistemos kontekstą.

● **Patikrinti hipotezę**, kad holistinis rizikų valdymas portfelio lygmenyje padidina rizikų valdymo efektyvumą, lyginant su rizikų valdymu atskirų projektų lygmenyje.

● **Pateikti rekomendacijų** sąrašą, kaip būtų galima padidinti rizikos valdymo brandą draudimo bendrovės projektų portfelyje.

Tyrimų metodika: šiame tyrime pasitelktas kokybinis tyrimo metodas, naudojant pusiau struktūrizuotus nuodugnius interviu, taip siekiant įvertinti draudimo bendrovės projektų portfelio rizikos valdymo brandos lygį ir nustatyti sritis, kurias reikia tobulinti. Pusiau struktūrizuotų interviu pasirinkimas grindžiamas tuo, kad jie leidžia išlaikyti balansą tarp struktūros ir lankstumo, iš anksto pasiruošus klausimų rinkinį, bet išlaikant galimybę pateikti nenumatytus klausimus ir ištirti netikėtas įžvalgas.

Rezultatai ir išvados: tyrimo išvados rodo, kad draudimo bendrovės projektų portfelio rizikos valdymo branda yra trečiame lygyje iš penkių, o iš dalyvių atsakymų išaiškėjo projektų portfelio rizikų valdymo sistemos spragos. Iš surinktų empirinių duomenų matoma, kad holistinis rizikų valdymas portfelio lygmenyje padidina rizikų valdymo efektyvumą, lyginant su rizikų valdymu atskirų projektų lygmenyje, nepaisant to, kad esamoje literatūroje vis dar trūksta išsamių tyrimų ir praktinių gairių projektų portfelio rizikų valdymui. Darbo išvadose pateikiamas praktinių rekomendacijų sąrašas organizacijos projektų portfelio rizikos valdymo sistemos tobulinimui.

Nors baigiamasis darbas teikia daugiausia naudos tarptautinei draudimo bendrovei, jis gali būti naudingas asmenims, studijuojantiems projektų portfelio rizikos valdymą (ar projektų valdymą apskritai), taip pat kitoms organizacijoms, kurios nori patobulinti savo projektų portfelio rizikų valdymą.

SUMMARY

VILNIUS UNIVERSITY BUSINESS SCHOOL

INTERNATIONAL PROJECT MANAGEMENT PROGRAMME

EMILIJA LEONOVAITĖ

ENHANCING PROJECT PORTFOLIO RISK MANAGEMENT AT AN INTERNATIONAL INSURANCE COMPANY

Supervisor: Vytautas Pugačevskis, Partn. Assoc. Prof.

Master's thesis was prepared in Vilnius, in 2024.

Scope of Master's thesis – 79 pages.

Number of tables used – 8 pcs.

Number of figures used – 4 pcs.

Number of references – 46 pcs.

Short description: project portfolio risk management is a potent concept, demonstrating the company's ability to consistently utilize risk management processes for achieving strategic objectives. Achieving a progressively higher project portfolio risk management maturity involves adopting an established framework, enabling organizations to measure themselves against recognized standards, providing a baseline for improvement and customizing approaches to address an organization's unique needs. However, this area is often overlooked in existing literature, as more attention tends to be given to risk management within individual projects.

Aim: evaluate the current risk management maturity of the international insurance company's project portfolio and identify framework gaps. Considering perspectives from organizational and portfolio-specific components, create a list of recommendations for improvement.

Objectives:

- To conduct an **in-depth literature review** on risk management practices within project portfolio, encompassing the broader context of the enterprise risk management framework, as well as components within the project portfolio.

- To **review existing risk management standards** and select the most suitable one for the study, complemented by an appropriate **maturity model**.
- To **assess the current risk management maturity level** of the project portfolio at the international insurance company and **identify gaps**, taking into account the broader context of the enterprise risk management framework and components within the project portfolio, and incorporating the chosen risk management standard and maturity model.
- **Test a hypothesis** that risk management within the portfolio governance allows a comprehensive approach to effectively manage risks compared to considering them within individual projects.
- To **provide a list of recommendations** for enhancing risk management maturity within the project portfolio.

Research methodology: this study employs a qualitative approach, utilizing semi-structured in-depth interviews to assess the maturity level of project portfolio risk management and identify areas for improvement. The choice of semi-structured interviews allows a balance between structure and flexibility, with a predefined set of questions and risk management maturity model criteria, while also allowing room for follow-up questions and exploration of unexpected insights.

Results and conclusions: the study findings indicate that the insurance company's project portfolio risk management maturity is at an intermediate Level 3 out of 5, and participant feedback highlighted several gaps in the company's risk management framework. The study emphasizes that risk management within the portfolio governance allows a comprehensive approach to effectively manage risks compared to addressing them individually in projects, despite a lack of tailored research and guidance in project portfolio risk management. The conclusion includes a list of practical recommendations to enhance the organization's project portfolio risk management maturity.

Whilst the thesis provides most benefits for the international insurance company, it may be useful for individuals studying project portfolio risk management (or project management in general), as well as other organizations that are interested in the enhancement of their project portfolio risk management maturity.

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

Relevance of the topic: the ability to manage risks is a fundamental organizational asset. However, to gain the most benefits, a mature risk management process is needed. Maturity encompasses more than just the formulation and execution of the process; it extends to the capabilities, expertise, and culture of the individuals utilizing it. To achieve maturity in risk management, organizations must adopt an established risk management standard, enabling organizations to evaluate their own risk management maturity, measuring themselves against established best practices. Furthermore, the journey towards higher maturity requires a pathway for improvement, not only revealing an organization's current position but also outlining the essential steps needed to ascend to the next level (Hopkinson, M., 2016). Generic standards alone, however, are insufficient; they must be tailored to suit the unique needs of each organization.

Research gaps: despite the extensive literature on risk management, there remains a notable absence of comprehensive research and practical guidance tailored specifically to risk management approaches designed for project portfolios. Existing literature tends to concentrate on risk management within individual projects, often sidelining the distinctive challenges posed by the project portfolio.

The central **research problem/question of the thesis** can be articulated as follows: how can risk management practices be further improved to evolve towards higher risk management maturity within the project portfolio at the international insurance company?

Research aim: evaluate the current risk management maturity of the international insurance company's project portfolio and identify framework gaps. Considering perspectives from organizational and portfolio-specific components, create a list of recommendations for improvement.

Research objectives:

- To conduct an **in-depth literature review** on risk management practices within project portfolio, encompassing the broader context of the enterprise risk management framework, as well as components within the project portfolio.
- To **review existing risk management standards** and select the most suitable one for the study, complemented by an appropriate **maturity model**.

- To **assess the current risk management maturity level** of the project portfolio at the international insurance company and **identify gaps**, taking into account the broader context of the enterprise risk management framework and components within the project portfolio, and incorporating the chosen risk management standard and maturity model.
- **Test a hypothesis** that risk management within the portfolio governance allows a comprehensive approach to effectively manage risks compared to considering them within individual projects.
- To **provide a list of recommendations** for enhancing risk management maturity within the project portfolio.

Research methodology: in the study, a qualitative approach was employed, utilizing semi-structured in-depth interviews to assess the maturity level of project portfolio risk management at the insurance company, identifying areas for improvement. The conceptual research model was composed based on the literature review, and influenced by the researcher's own understanding of how such kind of research should be carried out. Participants were selected using convenient sampling. The research was conducted with twelve respondents: a risk manager, head of strategy and project management division, four project managers and six subject-matter experts, each viewing the subject of the study from a different angle and providing a unique perspective.

Structure of the master's thesis: the master's thesis is structured into four parts. The initial section, dedicated to theory, is further subdivided into other two sections. The first one establishes the necessary context and offers key definitions essential for understanding the subsequent analysis, whilst the second section delves into an examination of existing risk management standards. This involves a selection process to identify the most suitable standard for the study with a corresponding maturity model to serve as a benchmark for assessing the maturity of the company's project portfolio risk management (that is subsequently detailed in the research results part).

The second part of the thesis outlines the research methodology, providing research questions, more context about the insurance company and a description of the research sample. Moving on to the third part, in-depth interviews with participants of the study are presented. These interviews unveil the maturity level of the organization's project portfolio, highlighting identified gaps where improvements are needed, with participants providing their suggestions for

improvements. In the final section, both theoretical and empirical research findings of the study are summarized and presented alongside practical recommendations on how the project portfolio risk management at the insurance company could be enhanced.

Difficulties and limitations: due to the nature of the study, there was a limited availability of comprehensive research and practical guidance written specifically about risk management approaches designed for project portfolios, which resulted in slightly fewer references used in the study.

1. CONTEXT AND KEY DEFINITIONS

1.1. Definition of risk

Various individuals or organizations may interpret risks in different ways. ISO Guide 73:2009 defines risk as “an effect of uncertainty on objectives. An effect is a deviation from the expected — positive and/or negative”. In the Standard for Risk Management in Portfolios, Programs, and Projects (PMI, 2019, p.7) and the PMBOK® Guide — Seventh Edition (PMI, 2021, p. 117), risk is “an uncertain event or condition that, when it occurs, can have either a positive or negative impact on one or more project objectives”. Both of these chosen definitions indicate that risks can manifest as either threats or opportunities. There are also three key attributes of a risk: uncertainty, the potential for loss, and a time component (Smith, P.G. and Merritt, G.M., 2002, p.5):

Uncertainty is inherent in risk management as there is a lack of certainty whether a risk will materialize or not. However, uncertainty can be mitigated by clarifying the risk's probability, understanding its consequences and factors that influence its likelihood.

It is crucial to distinguish between risks and certain events, which are known as issues (Becker, G. M., 2004; Westcott, T., 2005), although, both are relevant and should be documented. Risks involve the **possibility of experiencing a loss**, encouraging to manage them to avoid adverse outcomes, even though there is a chance that the risk will bring an unexpected benefit (which would make the risk positive).

Lastly, every risk has a **time component**, indicating when it will cease to exist (this distinguishes risks from other ongoing business concerns). It could be either when the loss occurs, or when the risk is resolved to a point where it no longer poses a significant threat.

1.2. Risk attitude

Risk attitude is “a chosen response to risk, driven by perception, and it can act as a control point to ensure that the right amount of risk is taken, so that the achievement of objectives is optimized” (Hillson, D., 2012). According to PMI (2019, p.9), risk attitude refers to how people or groups approach uncertainty - favorably or unfavorably -, taking corresponding actions. It also characterizes how a company deals with assessing, embracing, retaining, avoiding, or pursuing risks, from being cautious (risk-averse) to being risk-seeking.

Organizations aim to establish a consistent method for evaluating and responding to risk throughout their operations. However, individuals tend to have varying attitudes toward risk, which sometimes make it difficult to perform effectively (Jonas, V. & Chumber, S., 2011; Pritchard, C. L., 2002). Attitudes change over time, underlining the need for a comprehensive approach to risk management with constant improvement reviews.

1.3. Risk appetite

Whilst sometimes confused with risk attitude, risk appetite is "an internal tendency to take a risk in a given situation, and it reflects organizational risk culture and the individual risk propensities of key stakeholders" (Hillson, D. 2012). According to PMI (2019, p.9), risk appetite is "the degree of uncertainty an organization or individual is willing to accept in anticipation or a reward". Risk appetite provides direction for risk management, influencing the decision whether it is logical to take on certain risks and shaping the types of risks that should be pursued.

1.4. Risk threshold

The concept of risk appetite is expressed using risk thresholds – which can be described as a measure of tolerance around an objective, marking the point at which a risk becomes unacceptable, reflecting what kind of risk appetite an organization has (Hillson, D., & Murray-Webster, R., 2012, p.34; PMI, 2021, p.54). Risk thresholds are moderated by risk attitude to limit the impact of unmanaged risk appetite, ensuring that risk thresholds are set appropriately (Hillson, D. 2012).

Defining risk thresholds is a crucial step in connecting portfolio, program and project risk management to strategy alignment and should be done early in the planning phase (PMI, 2019, p.10). As per the Standard for Risk Management in Portfolios, Programs, and Projects, there are a few examples of thresholds:

- To be included in the risk register, there must be a threshold for a minimum level of risk exposure;
- Before triggering a risk escalation, there must be a threshold for a maximum level of risk exposure that can be managed;

- Qualitative (high, medium, low, etc.) or quantitative (numerical) definitions of risk rating (PMI, 2019, p.10).

1.5. Definition of risk management

Many internal and external risks affect organizations, and risk management is a process that helps understand and control these risks (Inclus, 2022). It could also be seen "as preparation for possible events in advance, rather than responding as they happen" (Pym, D. V., 1987). Risk management empowers organizations to systematically evaluate and control risks on multiple domains (i.e. enterprise, portfolio, program and project), supporting the realization of organizational objectives and strategic vision, and creating value (PMI, 2019, p.25). If not approached systematically or neglected, risk management may become a cumbersome process that does not fulfil its purpose (Inclus, 2022).

Risk management involves the processes of identifying, assessing, and addressing various risks within an organization (Inclus, 2022). Taking calculated risks ensures that a business invests in the right opportunities and grows, whereas effectively identifying and managing risks helps to avoid threats that could have a negative impact. It is important to create a risk management culture where employees understand the significance of monitoring and managing risks (Inclus, 2022).

However, risk management can be overdone, meaning that effective risk management requires effort and time that could be dedicated to product development (Smith, P.G. and Merritt, G.M., 2002, p. 12). The more mature the risk management process is, the more it will cost. It is crucial for the company to be able to pick the most critical risks that it will manage, based on their consequences and likelihood and on the cost of resolving them (Kutsch & Hall, 2009 as cited in Teller, J. et al., 2014, p. 67).

1.6. Risk management life cycle

Risk management is usually understood based on a life-cycle approach, being a iterative process that supports strategic decision-making. As per PMI (2019, p.29); Becker, G. M. (2004); Lavanya, N. & Malarvizhi, T. (2008), the risk management life cycle includes these elements:

- **The Risk Management Plan** describes the main risk management processes, providing a list of risk categories, covering (agreements about) resources, escalation paths, tools and

templates, methodologies, roles and responsibilities, review and reporting frequency, establishing risk terminology, thresholds, and other relevant values for effective risk management.

- **Risk Identification** is an iterative process, as risks can appear at any time. All detected risks are documented, with a risk owner assigned to treat and monitor them.
- **Perform Qualitative Risk Analysis** prioritizes and categorizes risks based on their significance and impact.
- **Perform Quantitative Risk Analysis** quantifies the overall impact of risk on objectives. However, its use is not compulsory.
- **Plan Risk Responses** determines actions to deal with risks, considering stakeholders' attitudes. Responses are planned at a strategic level.
- **Implement Risk Responses** involves defining approved actions and monitoring their effectiveness.
- **Monitor Risks** reevaluates identified risks, assesses risk management effectiveness, and triggers periodic risk reassessment.

1.7. Domains of risk management

Risks are managed across various governance layers, encompassing enterprise, portfolio, program, and project domains (PMI, 2019, p.21) – in other words, risk management spans all organizational levels, as presented at Figure 1.

At the enterprise level, the overarching strategy comprises of actions to encounter business threats and exploit opportunities. These actions are often executed within the portfolio components: programs, projects etc. All risk management policies and processes are customized to the project portfolio from the enterprise risk management framework, meanwhile, project portfolio components derive their risk management practices from the overarching portfolio framework (PMI, 2019, p.21).

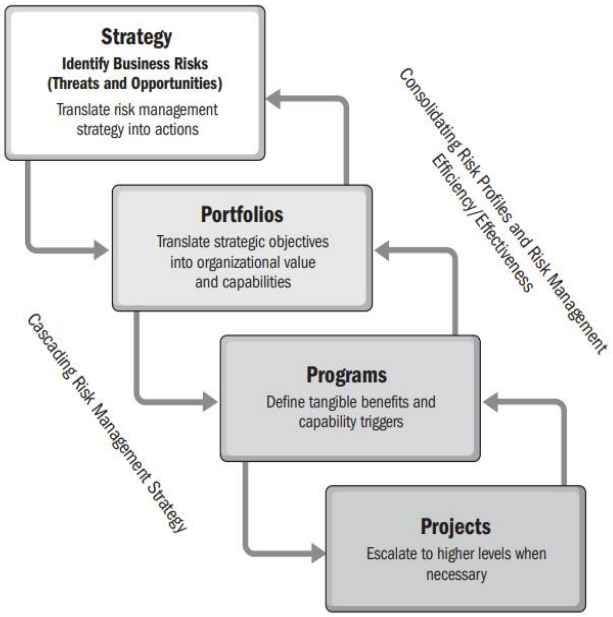

Figure 1. Cascading risk management strategy

Source: "The Standard for Risk Management in Portfolios, Programs, and Projects" (PMI, 2019, p.12).

In the sections below, three of the main organizational domains – portfolio, program and project - will be covered to gain a deeper understanding of the differences and accountabilities of each level.

1.7.1. Risk management in portfolios

According to PMI (2019, p.41), a portfolio is "a collection of projects, programs, subsidiary portfolios, and operations managed as a group to achieve strategic objectives". A key objective in portfolio management is to construct a portfolio that optimally manages risk, choosing to take the appropriate amount of risk by selecting or removing components considering their alignment with strategic objectives, the allocation of financial and human resources (Faris, R. K. & Patterson, D., 2007; PMI, 2019, P.41). The choice of components for the portfolio may arise in response to recognized threats or opportunities, aligning with the broader business strategy of the organization. In other words, the essence of portfolio management is to reduce overall risk through diversification by "not putting all eggs in the same basket" (Jamshidnejad, N., 2021, p. 219).

At portfolio level, risk management covers strategic, execution, and structural risks. This encompassing approach considers risks that have the potential to influence diverse components and operational functions within the portfolio. Furthermore, handling risk at the portfolio level presents several challenges, given that these risks span external and internal factors, linking organizational strategy with implementation (PMI, 2019, p.24 page). Additional risks typically addressed at the portfolio level encompass evolving business requirements, changes in the environment and context, resource availability, and the interplay and potential conflicts between different components.

1.7.2. Risk management in programs

The definition of a program given in "The Standard for Program Management"—Fourth edition (PMI, 2017, p.3) is "a group of related projects, subsidiary programs, and program activities managed in a coordinated manner to obtain benefits not available from managing them individually". Risk management at the program level assesses risks within interconnected/related components. It guarantees that these components implement efficient processes throughout the entire risk management life cycle, preventing any divergence between the program roadmap and its aligned objectives with the organizational strategy. This involves establishing risk thresholds for the program, conducting the initial risk assessment, formulating a comprehensive response strategy, and determining the communication protocols (PMI, 2019, p.49)

Risks relevant to the program risk management that can be identified at these levels:

- Risks coming from the portfolio or enterprise domains that may have an impact on program objectives;
- Risks identified directly at the program level, e.g., triggered by program interdependencies;
- Risks coming from the program components (Hillson, D. 2008; PMI, 2019, p.50).

1.7.3. Risk management in projects

According to the PMBOK® Guide—Seventh edition (PMI, 2021, p.4) the definition of a project is "a temporary endeavor undertaken to create a unique project service or result". Projects are inherently temporary and conclude upon reaching their specific objectives. Project risk management identifies and manages project risks that may have an impact on project's cost, schedule, or scope.

The primary objective of managing project risks is to enhance the likelihood and/or impact of opportunities while diminishing the likelihood and/or impact of threats, aiming to optimize project success. According to the PMBOK Guide (2021), if left unattended, these risks have the potential to derail the project from its plan and hinder the attainment of defined project objectives and benefits. As a result, the success of a project is intricately linked to the efficacy of project risk management (PMI, 2019, p.15).

The evaluation and analysis of risks happen at the tactical level, and all other risks that might have an impact on value delivery or benefit creation are escalated to overarching governance layers (PMI, 2019, p.57).

1.8. Risk management maturity

The level of maturity indicates how proficient an organization is in effectively employing consistent processes within one or more business areas. (Hartono, B. et al., 2019). The maturity of risk management in the project portfolio positively impacts the performance of the project portfolio, signifying the company's capability to consistently employ risk management processes to attain strategic objectives (Zanfelicce, R. L., & Rabechini, R., 2021). Mature organizations tend to have well-defined, standardized, and integrated processes and practices for managing risks, indicating the level of advancement attained in their operations.

To enhance risk management practices, an organization needs to follow a few steps as outlined below:

- Initially, an organization must ascertain which specific risk management practices have demonstrated consistent effectiveness in/by other organizations;
- Secondly, an organization requires a means to evaluate its current risk management state in comparison to these preferred practices;
- Thirdly, should an organization indeed embark on the path of enhancement, it must understand how to enhance itself in the identified areas requiring improvement (Fahrenkrog, S. L. et al., 2003). The improvement could be done utiziling a standard for benchmarking (Hartono, B. et al., 2019).

The concept of maturity suggests a potential progression from one level of capability to a more advanced one (Andersen, E. S. & Jessen, S. A., 2007), ranging from an initial (novice) level

to expert level, where risk management processes are being optimized. Advancing through these maturity levels entails the gradual improvement, refining the organization's risk management processes. Each level incorporates the criteria of the preceding one, fostering a more efficient and proactive approach to risk management (Proença, D. et al., 2017).

A prevalent approach to measure risk management maturity is to utilize a maturity model, that helps self-assess the existing level and pinpoint gaps and areas that require enhancement (OECD, 2021, p.5). Maturity models represent a path toward a more structured and systematic approach to conducting business, encompassing individuals, organizations, and processes. There has been a widespread adoption of such tools in recent years, extending across various domains like data management, information security, and project management. (Proença, D. et al., 2017).

Depending on the industry and the chosen risk management standard, there is a big selection of different maturity models. The most appropriate one for this study will be presented at the end of chapter 2, after a review of existing risk management standards.

1.9. Existing research on project portfolio risk management

Risk management at portfolio level can introduce an additional layer of organizational excellence, mitigating risks on future components and enabling continuous improvement. This is relevant to organizations involved in iterative development and those aspiring to elevate their (risk management) maturity. When viewed comprehensively, project portfolio risk management emerges as a potent concept, ensuring success in programs and projects while enhancing overall competitiveness in the organizational and business landscape (Bissonette M.M., 2016, p.4).

However, the available literature on risk management within project portfolios (or programs) highlights an intriguing aspect: up to this date, it is a relatively understudied domain compared to project management. While project risk management has received considerable attention, literature on portfolio risk management leaves room for further refinement and evolution (Teller, J., & Kock, A., 2013; Zanfelicce, R. L., & Rabechini Jr., R., 2021).

The gap between risk management practices within project portfolios and projects was already visible in late 2000s and early 2010s. Sanchez, H., et all (2009b) in the study “Risk Management Applied to Projects, Programs, and Portfolios" argued that at the time, it was difficult to find specific risk management guides or tools for project portfolios, arguing that from a strategic

perspective, this was an outstanding inconvenience because a project portfolio was the means to the transfer of strategic needs to its components and operational activities. At the time, project risk management standards were used at all levels. The paper exhibited an area of opportunity where methodologies and guides could be further improved to evolve towards better risk management structures.

Similarly, Micán, C., et al (2020) argued that in-between 2008 and 2014, a substantial part of the works focused on risk management in project portfolios merely demonstrated the importance of the area, whilst only in recent years there have been more specific proposals published which help to identify, categorize and assess project portfolio risks ("The Standard for Risk Management in Portfolios, Programs, and Projects", which was released in 2019 for the first time, is a very valuable reference). The paper pinpointed prospective avenues for future research. These include delving into project portfolio risk management as an integral component of organizational risk management, examining the success factors and strategic implications associated with project portfolio risk management, exploring mechanisms for project portfolio risk assessment, and understanding project portfolio risk management as a complex and dynamic system. Further research in these domains is crucial for cultivating a more insightful understanding of the challenges inherent in these areas. Concerning the success factors and strategic impact of project portfolio risk management, Arlt, M. (2010, p. 34) emphasized that additional exploration into enhancing portfolio risk management could significantly contribute to the overarching strategic success of project portfolios.

Moreover, it is also essential to recognize that a project in general is not isolated; it exists within the larger context of an organization, project portfolios, programs and the organization's strategic objectives (Martinsuo, M., & Anttila, R., 2022; PMI, 2019; Faris, R. K. & Patterson, D., 2007). This interconnectedness underscores the necessity for comprehensive risk management strategies that encompass the entirety of an organization's endeavors, highlighting an assumption that managing risks solely at the individual project level is inadequate and that a portfolio-wide perspective is needed (Teller, J., & Kock, A., 2013).

To compare portfolio risk management with project risk management, portfolio risk management offers several advantages: enhanced decision-making, providing a holistic perspective on risks across all projects, optimized resource prioritization to avoid inefficiencies,

stronger alignment with the organization's strategic objectives, enhanced agility and flexibility in responding to changes and unforeseen events, and higher stakeholder confidence (Kashkash, A., 2023; (Jamshidnejad, N., 2021, p. 219-220). Analyzing risks within the portfolio context aids in recognizing risks that could otherwise be perceived as standalone occurrences within specific projects, facilitating a thorough approach to risk mitigation. According to Jamshidnejad, N. (2021), Jamshidnejad, N. (2021), the absence of effective project portfolio risk management system frequently arises due to insufficient recognition of portfolio risks, a constrained overall perspective, inadequate expertise, time limitations, and difficulties in justifying the related expenses.

In conclusion, the significance of risk management within the project portfolio lies in its holistic approach. Effectively managing programs, multiple projects, and initiatives concurrently requires a comprehensive understanding of risk management, providing organizations with an overarching perspective. This approach allows for addressing risks that impact the entire portfolio rather than focusing solely on individual components, a crucial aspect in efficiently achieving strategic objectives. Furthermore, integrating risk management into project portfolios contributes to ensuring alignment with an organization's strategic goals. Rigorous research in this domain enhances organizations' capabilities to identify, prioritize, and manage risks that directly influence their strategic outcomes.

Furthermore, risk management is a dynamic, iterative process that responds to change. While generic risk management standards exist, the risk management process's context adapts to each organization's specific needs. Therefore, organizations must regularly review and improve their risk management policies and frameworks, responding to events or changes in circumstances (Lalonde, C. & Boiral, O., 2012, p. 279), and tailor the standards to meet their unique needs.

2. EXISTING RISK MANAGEMENT STANDARDS

Risk management has become a mature discipline with risk management standards being developed by different organizations to share best practices and specific norms based on accumulated research and experiences (Rampini, G. H. S. et al, 2019, p. 895). According to ISO/ IEC Guide 2 (2004, p. 10) a standard is "a document, established by consensus and approved by a recognized body, which provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context".

For the study, three risk management standards: ISO 31000, PMI's "Standard for Risk Management in Portfolios, Programs, and Projects" and COSO ERM were selected, compatible with the subject of the study. Chosen standards are also popular among risk management practitioners. Below, a brief description of the three selected standards is given, as this information will help determine which standard is best suited for the thesis topic.

2.1. ISO 31000 standard

One of the most important and recognized standards is the "31000 series - Risk Management (2018)" from the International Organization for Standardization (ISO). ISO 31000 is a consensual reference, that influenced certain organizations involved in developing risk management frameworks to re-assess their work against the standard. ISO 31000 offers a principles-based, versatile model applicable across industries and for various types of risks, irrespective of their nature (Perera, A. a. S., 2019, p.214). As a result, this resource does not dictate a specific risk management system but rather advocates for the support and integration of risk management into an organization's overall management system (Proença, D. et al. 2017).

The ISO 31000 standard is different from other ISO standards in that it is not certifiable (Vargas, D. B., & Campos, L. M. S., 2017, p. 1475). Regardless, while ISO 31000 does not officially mandate the utilization of audits, organizations are free to conduct periodic and independent evaluations of their risk management systems (Lalonde, C. & Boiral, O., 2012, p. 291). This practice contributes to maintaining a continuous improvement approach with risk management across the organization.

ISO 31000 stands out as an easily customized risk management standard. Operating primarily as a manual for devising and executing effective and organized risk management strategies, it offers eight principles and guidelines to guarantee its efficacy:

Table 1. ISO 31000 risk management principles

Best Available Information: effective risk management should be backed up by historical and current data, incorporating diverse perspectives and insights from experts within the organization. All gathered information should be documented and standardized (e.g., by grouping it into risk categories and adding new information on top) to have comparable data across operations.
Inclusive: to enhance reliability of risk assessments**,** relevant stakeholders should be involved in the process, in turn ensuring that the stakeholders are aware of identified risks.
Human and Cultural Factors: organizations should promote a culture of collective accountability for risk management, facilitating open discussions about risks, as this would help achieve higher excellence in the risk management process.
Integrated: risk management should span all organizational levels.
Structured and Comprehensive: arranging the framework for risk management activities ensures consistency, although it is advisable to not be overly rigid.
Customized: it is essential to customize risk management process and risk activities documentation to the unique needs of each organization.
Dynamic: effective risk management should be highly adaptable to swiftly respond to any changes in business environments.
Continuous Improvement: risk management necessitates continual evaluation and improvement due to internal and external changes in organizational context.

Source: adapted from "ISO 31000 principles explained – handbook for effective risk management" (Inclus, 2022) and "ISO 31000:2018 Risk management — Guidelines" (ISO, 2018).

In conclusion, ISO 31000 had a significant impact on organizations seeking to align their risk management structures. These risk management principles can guide internal auditors in selecting audit areas and assessing audit evidence (Moeller, R., 2016, p. 149), ensuring a holistic and effective approach to risk management within different domains at an organization.

2.2. PMI's "Standard for Risk Management in Portfolios, Programs, and Projects"

Another acknowledged standard comes from the Project Management Institute (PMI), which is the leading professional association for project management. PMI released many global standards over the years, thriving to achieve excellence in the field of portfolio, program and project management. In 2019, PMI released "The Standard for Risk Management in Portfolios, Programs, and Projects", which describes the main concepts and definitions associated with risk management, highlighting the interconnectedness between various governance layers: enterprise, portfolios, programs, and projects. The standard describes the fundamentals of risk management by linking it to enterprise risk management (covered in the first chapter of this study, the "Context and Key Definitions" part) and risk management principles relevant to portfolio, program, and project domains (covered in the sections below).

2.2.1. Core principles

PMI's offers a comprehensive risk management framework; one part of the framework, similarly to ISO 31000, emphasizes those principles that are fundamental to effective and successful risk management:

Table 2. Risk management principles from the Standard for Risk Management in Portfolios, Programs, and Projects

Strive to achieve excellence in the practice of risk management: risk management helps organizations enhance the predictability of outcomes and stability of organizational performance.

Align risk management with organizational strategy and governance practices: risk management should adapt to changes in organization's strategy and governance.
Focus on the most impactful risks: it is essential for organizations to be able to prioritize risks based on their impact, ensuring proper resource allocation to deal with the most relevant risks.
Balance realization of value against overall risks: there should be a balance between exposure to risk and realization of business value.
Foster a culture that embraces risk management: organizations should thrive to have a high risk-awareness among its employees, so that both threats and opportunities are recognized and treated and not neglected.
Navigate complexity using risk management to enable successful outcomes: risk identification and management leads to optimized resources, increasing returns on investments, and the overall improvement of organizational performance.
Continuously improve risk management competences: to achieve higher risk management maturity and strengthen organizational performance, there should be a constant review and refinement of the risk management process.

Source: adapted from the "Standard for Risk Management in Portfolios, Programs, and Projects" (PMI, 2019, p.3-5).

2.2.2. Integration of RM practices into portfolio, program, project management

To attain the project portfolio's objectives, several risk management practices that can be utilized across the portfolio life cycle. Since a project portfolio consists of programs and individual projects, the performance domains and process groups of all the three domains are covered below for context:

Table 3. Performance and process domains at portfolio, program and project levels

Project portfolio level	Program level	Project level
Portfolio strategic management	**Program strategy alignment**	**Initiating processes**
Ensuring that opportunities are seized and threats are addressed at a strategic level.	Aligning programs with the organizational strategy and handling strategic opportunities and threats, making redefinition or adjustment of program elements where needed.	Establishing projects or phases, ensuring that high-level risks are identified before authorization.
Portfolio governance	**Program governance**	**Planning processes**
Ensuring adherence to legal and regulatory requirements, risk management acts as a protective measure against misconduct.	Controlling programs to be aligned with organizational goals, integrating risk management practices (e.g., risk escalation process).	Alongside the setting of project scope and objectives, the organization selects a risk management approach, to ensure integrity and quality of the project.
Portfolio capacity and capability management	**Program life cycle management**	**Executing processes**
Ensuring that the (human) capital entrusted to the portfolio and its components is properly used.	Adding the right components to the program in the right sequence, aligned with the program's business case, identifying and addressing program-level risks as early as possible.	Aiming to fulfill project objectives/requirements and ensuring effective risk management process.
Portfolio stakeholder engagement	**Program stakeholder engagement**	**Monitoring and controlling processes**

Ensuring active involvement of stakeholders at the portfolio level to contribute positively to the realization of the organization's strategy.	Ensuring active involvement of stakeholders at the program level.	Monitoring, assessing, and managing the progress and performance of the project.
Portfolio value management	**Program benefits management**	**Closing processes**
Ensuring the delivery of expected value.	Ensuring the delivery of expected benefits (and other objectives).	Officially concluding the project, securing collected knowledge.
Portfolio risk management	**Supporting program activities**	
Ensuring effective management of risks at the portfolio and its component levels.	Ensuring comprehensive program activities coverage through risk management practices.	

Source: composed by the author based on the "Standard for Risk Management in Portfolios, Programs, and Projects" (PMI, 2019, p. 45-63).

2.3. COSO enterprise risk management standard

The third standard examined in the study is the COSO (Committee of Sponsoring Organizations of the Treadway Commission) ERM, initially developed as an enterprise risk management (ERM) model in 1992, represented as a pyramid with a focus on evaluating existing controls. In 2013, it was transformed into the COSO cube, giving emphasis to the design and implementation of a risk management framework. The COSO cube gained broad acceptance, proving to be a versatile model in various global contexts. In 2017, the cube was updated into a helix structure, however, the COSO cube maintained its popularity and continued to be valuable as it provides a framework for enhancing risk management and internal control (IRM, 2018, p. 4,10), allowing an enterprise and internal audit to consider and assess risks at all levels (Moeller, R., 2016, p. 113).

The COSO ERM framework seeks to provide a model for enterprises to consider and understand their risk-related activities across all domains, including the interplay of these risk components:

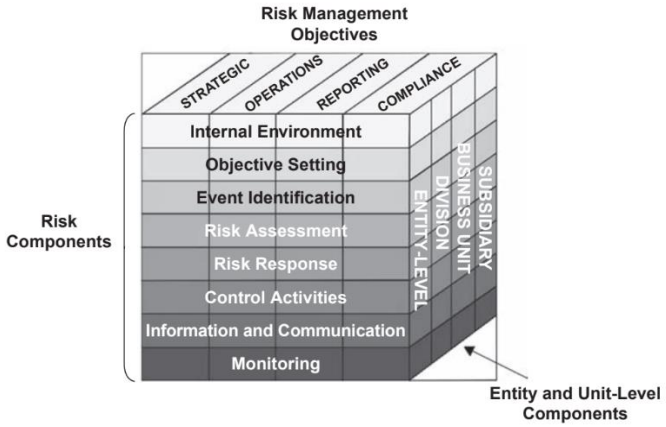

Figure 2. COSO ERM Framework

Source: Brink's Modern Internal Auditing (2016, p.156)

As seen in Figure 2, COSO three-dimensional cube has the following components:

- Strategic objectives of enterprise risk are represented in vertical columns.
- Risk components are shown in the horizontal rows.
- Levels to describe any enterprise (subsidiary, business unit etc.), depending on the organization's size.

Table 4. COSO ERM risk management components

Internal environment: the board's influence shapes the organizational tone, affecting risk appetite, perspectives on risk management, and ethical values.
Objective setting: the board sets objectives in accordance with the organization's mission and risk preferences, evaluating potential risks associated with the pursuit of different goals and ensuring alignment between risk tolerance and risk appetite.

Event identification: recognizing events that influence their objectives, organizations must distinguish between adverse risks and favorable opportunities. It's essential to tackle both operational and strategic risks.
Risk assessment: it is important to have a structure to analyze risks probability, consequences, and interconnections.
Risk response involves selecting actions aligned with risk tolerance and appetite, typically categorized as reduce, accept, transfer, or avoid. It is essential to evaluate risks at the enterprise level, considering regulatory requirements, costs etc.
Control activities encompass policies and processes designed for effective responses to risks.
Information and communication: there must be timely data identification and communication between stakeholders, ensuring that employees meet their responsibilities and that there are no delays of potential issues escalation to upper management.
Monitoring: there is a need for regular monitoring and adjustments, with regular audits as organizations expand in size and complexity over time.

Source: adapted from Brink's Modern Internal Auditing (2016, p. 157-171).

In summary, the COSO Enterprise Risk Management (ERM) standard enables organizations and internal audit teams to comprehensively evaluate risks across all levels, recognizing their interconnectedness and impact on strategic objectives. By following the principles outlined in the COSO ERM framework, companies can synchronize their risk management approaches with strategic goals and values, thereby improving risk mitigation and governance. This framework proves exceptionally beneficial in heightening risk awareness and proactively addressing risks to avert potential adverse consequences.

2.4. Evaluation of the standards

Selecting the right risk management standard is critical for improving the risk management in an international insurance company's project portfolio. In this context, ISO 31000 stood out for several reasons:

The standard has global recognition and is known to the international insurance company, as the company's claims administration quality system is benchmarked against the LST EN ISO 9001:2008 standard and the organization is in the process of obtaining another ISO-certification (details cannot be shared due to confidentiality). ISO 31000 is an easily adaptable, generic standard, offering the flexibility to tailor risk management to the organization's unique needs, crucial in the diverse landscape of insurance. Therefore, ISO 31000 was considered as the best option to align the company's project portfolio risk management practices with global best practices, ensuring credibility and instilling stakeholder confidence in the study's results.

Moreover, ISO 31000 benefits from a wealth of publicly available resources, making knowledge dissemination and implementation easier. It is also well-supported by maturity models, which made it easier to find and select the appropriate one, utilizing it to evaluate the risk management maturity level at the organization, providing the baseline for improvement.

Generally, ISO 31000 is regarded as an effective framework, even though "many organizations tend to adopt ISO standards quite superficially in order to reinforce their social legitimacy through the implementation of rational and reassuring frameworks" (Lalonde, C. & Boiral, O., 2012, p. 273). The implementation of the COSO ERM standard might present challenges attributed to its intricate nature, difficulties in customization, and a perceived lack of clarity. Some organizations might find the language and the terminology used in the COSO ERM framework to be too abstract and/or lacking practical guidance. Tailoring the COSO ERM framework to an organization's specific needs and risk profile could be challenging, as organizations may struggle to determine which components of the framework are most relevant to them and how to adapt them effectively. This could lead to confusion and difficulty in translating the framework into actionable steps.

Implementing "The Standard for Risk Management in Portfolios, Programs, and Projects" would also come with its challenges due to its complexity, a lack of maturity models and resources publicly available to back up the standard. Whilst this standard fulfills a business need to provide guidance for risk management practitioners in portfolio, program and project management domains, there is a lack of critical evaluations of this standard to explore its possibilities and limitations. On the other hand, the standard is extremely valuable in the sense that it was written specifically for portfolio, program and project management domains.

2.5. Risk management maturity model

Establishing effective risk management processes can pose challenges, and numerous organizations encounter difficulties in attaining their intended results. However, utilizing a risk management standard with a complementing maturity model simplifies the process.

In this study, a maturity model based on ISO 31000 (drawing inspiration from its risk management principles) was selected, taken from the study by Proença, D. et al. called "Risk Management: A Maturity Model Based on ISO 31000, 2017", designed to assess an organization's current level of risk management maturity. As part of the process for implementing risk management, organizations need to define the context and identify areas where domain-specific risk management practices, methods, or techniques are required (Proença, D. et al. 2017). The insights garnered from this evaluation form the basis for constructing a set of recommendations aimed at steering organizations toward their desired maturity level. This maturity model not only enables organizations to assess their risk management practices in comparison to established best practices in the industry but also serves as a guide for enhancing their risk management processes.

The selected model acknowledges the need for flexibility and adaptability across a variety of organizations and industries. However, like any model, it has its limitations. The authors recommend ongoing evaluation, adaptation, and refinement of the RM maturity model, especially when applied to different industry sectors. It is also important to note that beside utilization of the maturity model, PMI's "Standard for Risk Management in Portfolios, Programs, and Projects" will be used as a reference to bridge any potential gaps that might not be covered by the maturity model alone.

As per the Table 5 below, the model suggests the following maturity levels: Level 0 – Non-existent RM; Level 1 – Initial RM; Level 2 – Managed RM; Level 3 – Defined RM; Level 4 – Quantitatively Managed RM; Level 5 – Optimizing RM.

To progress through maturity levels in risk management:

- Transition from Level 0 to 1: The organization recognizes the necessity for a risk management process but primarily operates reactively.

● Progress from Level 1 to 2: Attempts made to align risk management activities with the policy established by stakeholders, yet the process is influenced by past "habits" rather than adhering to a formalized approach.

● Advancement from Level 2 to 3: The risk management process becomes standardized and integrated into organizational activities.

● Shift from Level 3 to 4: Quantitative and statistical methods are used for risk management process.

● Transition from Level 4 to 5: Refinement of the established risk management practices.

According to Proença, D. et al. (2017), progression through these stages entails fulfilling the requirements specific to each level, leading to more resilient and clearly defined risk management processes that contribute positively to the achievement of organizational strategic plans. As organizations undertake the process of enhancing their risk management maturity, they can anticipate increased resilience, refined decision-making, and overall improvement in organizational performance. The maturity level assessment criteria are represented below (minimally edited by the author of this study):

Table 5. Visual representation of the Risk Management Maturity Model

Level 5 - Quantitatively Managed
5.1 Systematically identify areas for improvement. *5.2* Thoughtfully select and implement improvements. *5.3* Rigorously evaluate the effects of implemented improvements. *5.4* Investigate causes leading to selected outcomes. *5.5* Systematically address causes of selected outcomes.
Level 4 - Optimizing
4.1 Establish and maintain process quality and performance objectives. *4.2* Employ measures and analytic techniques for quantitative risk management.

4.3 Analyze process performance systematically.

4.4 Set up process performance baselines.

4.5 Regularly report risk management performance comprehensively.

Level 3 - Defined

3.1 Provide training in risk management throughout the organization.

3.2 Integrate risk management seamlessly into all organizational processes, including project portfolio and program management.

3.3 Identify responsibilities for risk management at every organizational position.

3.4 Ensure all identified risks have an assigned owner.

3.5 Ensure risk management practices comply with regulatory and legal requirements.

3.6 Identify and record stakeholders' perceptions, considering them in decision-making.

3.7 Ensure communication and consultation are integral to all risk management activities.

3.8 Take account of both the internal and external context when it comes to risk management.

3.9 Align risk management goals and objectives with organizational objectives (i.e., minimizing losses, optimizing resource allocation etc.).

3.10 Systematically find, recognize, record and describe risks.

3.11 Determine risk levels and compare them with predefined criteria.

3.12 Prioritize risks for treatment based on strategic considerations.

3.13 Develop a procedure to identify potential positive risks.

3.14 Identify risks associated with not pursuing opportunities.

3.15 Study interdependence between different risks and their sources.

3.16 Incorporate cost/benefit analysis for each risk treatment option.

3.17 Identify, communicate, and monitor secondary risks.

3.18 Record, monitor and review all risk management activities comprehensively.
Level 2 - Initial
2.1 Assign dedicated individuals to specific roles in risk management. *2.2* Ensure adequate resources are available to support risk management activities.
Level 1 - Managed
1.1 Initiate basic risk management reporting practices.

Source: adapted from "Risk Management: A Maturity Model Based on ISO 31000, 2017, Section 5"

It is important to note that the original risk management maturity model prepared in the "Risk Management: A Maturity Model Based on ISO 31000, 2017" study has more criteria. However, to avoid overburdening participants with excessive and potentially less relevant information, some criteria with overlapping meanings were excluded from this study, prioritizing only those criteria that were deemed relevant for the insurance company. These assessment criteria were used to evaluate the insurance organization's current state of risk management against identified best practices, offering insights into existing strengths and areas for improvement. A recommendations list was crafter in the conclusions part of the study, customized to target the specific areas in need of enhancement, aligning with the organization's available resources.

3. RESEARCH METHODOLOGY

3.1. Research model

The conceptual research model for this study was composed based on the literature analysis and is presented in Figure 3. Risk management maturity was studied utilizing the maturity model in Table 5 and evaluating the integration of risk management processes within the performance domains of portfolio management, considering different perspectives of the employees working at the insurance company.

Given the prevailing tendency in existing literature to focus predominantly on risk management within individual projects, often overlooking the overarching risk management within a project portfolio, a decision was made to test a hypothesis that risk management within the portfolio governance allows a comprehensive approach to effectively manage risks as it is not sufficient to consider risks in individual projects alone (Olsson, 2008 as cited in Teller, J. et al., 2014, p. 67). The underlying assumption is that a transition toward stronger project portfolio risk management would yield positive impact on decision-making, strengthen communication among key stakeholders and resource allocation, and improve prioritization and rationalization of chosen business changes (Faris, R. K. & Patterson, D., 2007) and that project portfolio risk management is not simply a collection of individual projects' risk management techniques. Ultimately, this approach is expected to contribute to bridging the existing gap about project portfolio risk management in literature and practice.

Research Aim:

- Evaluate the current risk management maturity of the international insurance company's project portfolio and identify framework gaps. Considering perspectives from organizational and portfolio-specific components, create a list of recommendations for improvement.

Objectives to be covered:

- To **assess the current risk management maturity level** of the project portfolio at the international insurance company and **identify gaps**, taking into account the broader context of the enterprise risk management framework and components within the project portfolio, and incorporating the chosen risk management standard and maturity model.

- **Test a hypothesis** that risk management within the portfolio governance allows a comprehensive approach to effectively manage risks compared to considering them within individual projects.
- To **provide a list of recommendations** for enhancing risk management maturity within the project portfolio.

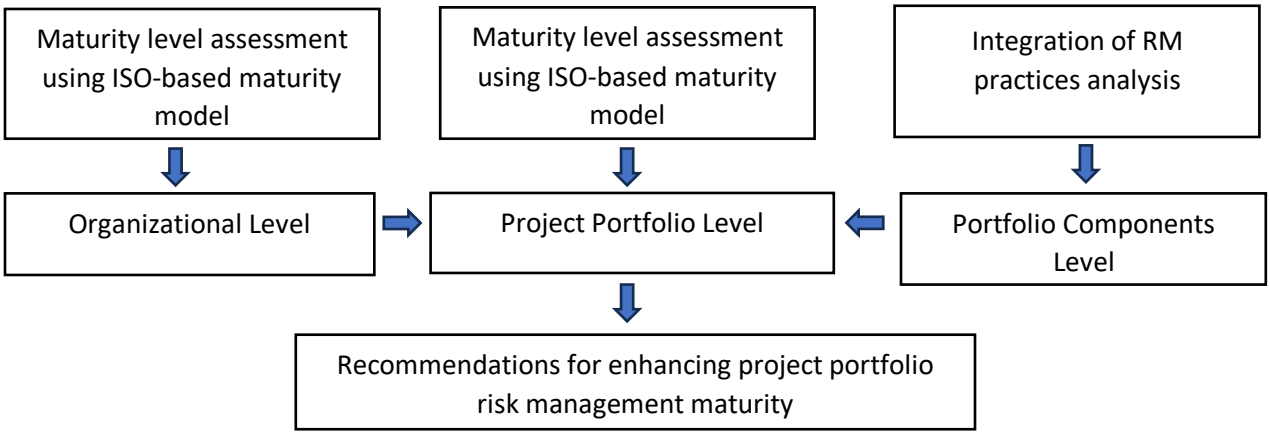

Figure 3. Conceptual model

Source: composed by the author

3.2. Research Sample

The selected insurance company operates within Scandinavia and the Baltics. Its offices in the Baltics are considered as a separate unit with around 600 employees, its own management, and the CEO, with upper management at the Baltics level reporting to the steering board in Scandinavia once per month. In the study, only the Baltics part of the company was analyzed, due to researcher's employment location and the company's corporate structure.

Within the Baltics, there is only one department for Strategy and Project Management, which oversees projects in the whole Baltics region. The department is relatively small, employing a few people. When projects are approved, employees from other departments are usually appointed as temporary project leads/managers.

In 2022 and 2023, the company had a strong focus on transformation and had an ongoing program consisting of 5 big change projects. Therefore, the portfolio consisted mostly of the program and had a couple of smaller projects running in the background, with the priority given

to the transformation program. The progress of the transformation program was reported directly to the steering board in Scandinavia every month, whilst the progress of smaller projects was usually discussed between the management members at the Baltic level. The Head of Strategy and Project Management Division oversaw both the portfolio and program management. At the end of 2023, a decision was made to officially close the program and several individual projects were approved. Therefore, it is important to note that due to the portfolio's structure in 2023, "transformation program" is mentioned many times in this study due to its importance at the company.

For the study, 12 employees from the company were selected using convenience sampling, ranging from individuals in risk management, strategy and portfolio management, project management roles, and other relevant personnel – each contributing to project portfolio activities to varying degrees. As participants have different backgrounds and fields of expertise, this ensures a versatile array of perspectives, enhancing the depth of the study. In regard to other relevant personnel, those individuals that possess a comprehensive understanding of an entire individual project scope and/or are preferably involved in multiple projects were chosen as participants in this study.

Participant information is provided below; however, due to confidentiality, the names of the participants are not mentioned, and only the roles of the main participants are mentioned, whilst many other participants expressed a wish to remain fully anonymous, therefore, they were marked as SME etc. (SME meaning Subject-Matter Expert):

Table 6. List of participants

RM	Risk manager
PPM	Head of Strategy and Project Management Division
PM1	Project Manager
PM2	Project Manager
PM3	Project Manager

PM4	Project Manager
SME1	Subject-Matter Expert
SME2	Subject-Matter Expert
SME3	Subject-Matter Expert
SME4	Subject-Matter Expert
SME5	Subject-Matter Expert
SME6	Subject-Matter Expert

Source: composed by the author

3.3. Research Method and Questions

This research employs a qualitative approach, specifically semi-structured in-depth interviews to investigate the project portfolio risk management maturity level and the existing gaps that need improvements. Semi-structured interviews were chosen as they provide structure and allow flexibility (Ruslin et al., 2022); for the research, a predefined set of questions was prepared together with the risk management maturity model criteria with flexibility for follow-up questions and exploration of unexpected insights. Some additional questions for subsequent participants were created after the initial assessment and questionnaire with the Risk Manager and the Head of Strategy and Project Management Division – the primary participants of the survey – in case they had any questions that needed answers from the following participants.

The way that the research was carried out is multifaceted:

- The first part is dedicated to evaluating the current risk management maturity level of the organization together with the risk manager using the ISO 31000-based maturity model in Table 5. Apart from the maturity model assessment, the Risk Manager was asked to provide their perspective on what should be improved within the project portfolio in regard to risk management.

- The second part focuses on evaluating the current risk management maturity level of the project portfolio together with Head of Strategy and Project Management Division using the ISO 31000-based maturity model in Table 5, backed up by a questionnaire set up using the key performance domains of project portfolio management.
- The third part is aimed at evaluating the integration of risk management practices in project portfolio components, with two separate questionnaires prepared: one for project managers, another one (consisting only of 2 questions) for other stakeholders who have a holistic approach to project portfolio components. Questions for project managers and subject-matter experts were created by the researcher, based on the questionnaire prepared for the Head of Strategy and Project Management Division, basically aiming to gather diverse perspectives on the same matters. Some comments made by the Risk Manager during the interview phrase were also turned into questions for Project Managers (the flow of thinking can be seen in the research results section).

All questions prepared by the researcher are open-ended, meant to get more insights about the current risk management practices. The project portfolio risk management practices were analyzed from different angles, taking into account the risk management practices at the organization as a whole, the project portfolio level, and project portfolio components' angle to see the full picture.

Part 1. Organizational level.

Assessment of the current risk management maturity level of the organization:

Questions for the Risk Manager:

- Undertake an assessment of the criteria outlined in Table 5 of the maturity model, identifying elements that apply to the organizational risk management.
- Identify gaps within the current framework and contemplate the potential value of their integration.
- Open-ended question – please provide your insights on what should be improved within the project portfolio in regard to risk management.

Part 2. Project Portfolio Level.

Assessment of the current risk management maturity level of the project portfolio:

Questions for the Head of Strategy and Project Management Division:

- Undertake an assessment of the criteria outlined in Table 5 of the maturity model, identifying elements that apply to project portfolio risk management.

Important to note that the following risk management maturity model criteria were removed in Part 2, as they were deemed relevant only for Part 1 (to the risk manager): *3.1.* Provide training in risk management throughout the organization; *3.2* Integrate risk management seamlessly into all organizational processes, including project portfolio and program management; *3.3* Identify responsibilities for risk management at every organizational position; *3.5* Ensure risk management practices comply with regulatory and legal requirements.

- Identify gaps within the current framework and contemplate the potential value of their integration.

Integration of risk management processes into portfolio management:

Questions for the Head of Strategy and Project Management Division:

Strategy (please briefly comment the following point for context):

- How are strategic opportunities identified and evaluated?

Governance:

- Are there specific policies or guidelines that guide risk management within the portfolio governance framework?
- Are there mechanisms for continuous improvement in portfolio governance practices related to risk management?

Capacity and Capability Management:

- What are the biggest challenges when it comes to resource allocation within the portfolio?

Stakeholder Engagement:

- What are the main risks related to stakeholders/stakeholder engagement within the portfolio?

Expected Value Delivery:

- How does the portfolio maximize opportunities to increase value?

Portfolio risks management:

- How satisfied are you with the timeliness of reporting on emerging risks by portfolio component leads?
- Are there established criteria for determining when a risk should be included in the risk register or escalated to higher levels within the organization?
- Is there a repository where systematic risks are identified, documented, and reviewed across the entire portfolio?
- Can you describe instances where and how lessons learned from past risks were applied to enhance future risk management?

Concluding question:

- Which specific risk management practices do you think could be strengthened, and what suggestions do you have for improvement?

Part 3. Project Portfolio Components Level.

Questions for Project Managers

Risk-awareness assessment:

- How much attention is usually given to risk identification and assessment within your project(s)?
- In your opinion, how well is the culture of shared responsibility for risk management established within your project(s)? Have you had any risk assessment sessions together with the project team(s)?

Assessment of risk reporting:

- Do you ensure the comprehensive inclusion of relevant risks in the risk and issue register? Is it clear for you how they should be categorized/prioritized based on their impact?

Dependencies between components

- What dependencies does your project have on other projects within the portfolio? How are you managing these dependencies and ensuring that they do not become risks/issues?

Resource allocation between components

- In your opinion, does the project portfolio have an adequate allocation of resources to its components?

Risk mitigation

- Can you share an example of successfully mitigated risk(s)? What role does planning a time buffer or creating a contingency plan play in your overall risk mitigation strategy?

Risk escalation

- Are you satisfied with how leadership is managing and resolving escalated risks?

Current risk management framework evaluation

- In your opinion, does the project portfolio have a satisfactory risk management framework?

Suggestions for risk management framework improvements

- Do you have any suggestions on how the project portfolio risk management framework could be improved?

Questions for Subject-Matter Experts:

- Based on the current project(s)/program(s) that you are a part of, which risks or issues do you consider as the main ones which are likely to recur next year/in new projects/programs?
- Are you satisfied with the progress of projects/programs within the company, and do you believe that the company achieves its goals successfully?

3.4. Data gathering and analysis

The interviews with participants were conducted face-to-face and through virtual meetings, recording the conversations with participants' approval. Interviews with participants in Part 1 and Part 2 lasted for around two and a half hours each. In Part 3, interviews with project leads took around 1 hour each, and with other stakeholders – around 15/20 minutes each, some of these participants also submitted their answers in a written form. All of the participants received the questionnaires in advance and had time to contemplate on the topics.

The data gathering and analysis process involved the following steps:

- All interviews from recorded sessions were transcribed.
- Responses were edited if they contained any confidential information.
- Responses were edited to only have valuable text.
- Interviews conducted in Lithuanian language were translated to English language by the researcher.
- Responses were analyzed and compared to see relevant patterns.

It is important to note that as many interviews were conducted in the Lithuanian language, the responses were edited to only contain valuable information before translation. Therefore, it was decided to include all answers in the research results part instead of annexes.

Research results are presented the third chapter of this study in the following order:

- 3.1. Section analyzes risk management maturity level of the organization.
- 3.2. Section analyzes risk management maturity level of the project portfolio.
- 3.3. Section analyzes the integration of risk management practices in the project portfolio components.
    - 3.1.1. Analysis of project managers' perspectives.
    - 3.3.2. Analysis of subject-matter experts' perspectives.

4. RESEARCH RESULTS

4.1. Risk management maturity assessment at organizational level

In this section, the maturity of risk management practices at the organizational level within the international insurance company is explored. The exploration seeks to provide a comprehensive understanding of how the company perceives and manages risks on a broader scale. This holistic perspective is crucial for effectively aligning the risk management strategies of the project portfolio with the overarching risk management strategy of the entire organization.

Together with the risk manager, it was established that the organization surpassed both Level 1 and Level 2 of risk management maturity, therefore, this section proceeds to conduct a more in-depth analysis of Level 3 criteria. The following comments offer insights into the evaluation of Level 3 maturity, shedding light on the organization's progress and areas for further enhancement in its risk management practices:

Table 7. Risk manager's answers in the risk management maturity assessment at organizational level

Level 3 - Defined
3.1 Provide training in risk management throughout the organization. *"**Yes**, generic risk management trainings are done once per year in each country (LT, LV, EE). Risk management trainings are also conducted specifically for new hires whenever the company has "rookie days". There are no risk management trainings or workshops specifically tailored for project managers".*
3.2 Integrate risk management seamlessly into all organizational processes, including project portfolio and program management. *"**Partially/more towards no**, whilst the risk manager conducts the risk assessment session at the organizational level, (s)he is not involved in risk management activities/risk assessments within the portfolio and is not familiar with what kind of documentation the portfolio has for risks management activities. Moreover, the risk manager is not fully aware what kind of projects the company has in its portfolio and what their content is. We know that there is a gap in the process which needs to be analyzed further".*

3.3 Identify responsibilities for risk management at every organizational position. *"**Yes**, we have risk owners and the company has a bottom up approach, valuing experts' judgement when it comes to risks. Once input is collected, the summary is given to the upper management".*

3.4 Ensure all identified risks have an assigned owner. *"**Yes**".*

3.5 Ensure risk management practices comply with regulatory and legal requirements. *"**Yes**".*

3.6 Identify and record stakeholders' perceptions, considering them in decision-making. *"**Partially**, whilst stakeholders' perceptions are identified and recorded, they are not always considered in decision making. The company does not have many examples when a risk-based decision was made at the organizational level".*

3.7 Ensure communication and consultation are integral to all risk management activities. *"**Partially,** all of the interactions are ad-hoc and there are no routine communications or consultations among internal employees at the Baltic level in regard to risk management activities. However, we have routine communication with the steering board that is located in Scandinavia every quarter about major (red) organizational risks, as we are legally required to report to the board every quarter".*

3.8 Take account of both the internal and external context when it comes to risk management. *"**Yes**, both internal and external contexts are considered, but there is a stronger focus on internal context/the assessment of internal risks and incidents. The company conducts the assessment of external risks at least once per year when it evaluates strategic risks. Regarding external risks, the initial step involves reviewing all emerging risks in the market. Subsequently, strategic risks are modeled based on the insights gained from this assessment".*

3.9 Align risk management goals and objectives with organizational objectives. *"**Yes**, there are key risk indicators (KRIs) that are aligned with the company's strategy/annual goals".*

3.10 Systematically find, recognize, record and describe risks. *"**Partially**, as we do recognize, record and describe, but we do not do it systematically. However, we could*

(and will) have a routine regarding IT risks. Digital Operational Resilience Act (DORA) within the EU requires a comprehensive information and communication technology (ICT) risk management framework for finance companies – and as insurance business is affected by this regulation, we will have to become fully compliant as well until 2025".

3.11 Determine risk levels and compare them with predefined criteria. *"**Yes**, we have a matrix with risk levels and predefined criteria. At organizational level we have definitions in the risk matrix: financial ranges, impact on customer satisfaction/reputation of the company, regulatory compliance, and risk handling rules for each risk level".*

3.12 Prioritize risks for treatment based on strategic considerations. *"**Yes**, the same matrix is used for risks prioritization".*

3.13 Develop a procedure to identify potential positive risks. *"**No**, there is no such process to identify opportunities. Our offices in Scandinavia have started to differentiate risks into upstream and downstream risks, however, on the Baltic level we only track negative risks at the moment".*

3.14 Identify risks associated with not pursuing opportunities. *"**Not really**, but it could be because we do not have many investment-based decisions (no mergers and acquisitions (M&A), for example)".*

3.15 Study interdependence between different risks and their sources. *"**No**, we combine similar risks into one and we do not analyze interdependencies".*

3.16 Incorporate cost/benefit analysis for each risk treatment option. *"**Partially**, whilst the company tries to incorporate cost/benefit analysis, it is not used for each risk treatment option. As an example, in the operational risk management policy, we have a statement that if the risk is "yellow"/mid-level, the risk owners decide themselves what to do with it and a cost/benefit analysis is not required. However, everyone understands that it should be worth to mitigate risks, therefore, we evaluate what is the best way for us to move forward".*

3.17 Identify, communicate, and monitor secondary risks. *"**No**, we do not have a definition of what a secondary risk is – and if such risks (would) appear, we (would) track them as new, separate risks".*

3.18 Record, monitor and review all risk management activities comprehensively. *"**No**, we do not have comprehensive reporting when it comes to risks. The company does not use an advanced risk management system, all risks and risk management activities are simply tracked in an excel with a focus on major/critical risks. Therefore, there is no written information about smaller risks, and we always update the same file without keeping an older copy in our archives, therefore, we do not have any historical information".*

Source: composed by the author

Based on the assessment of the maturity model criteria, it was determined that the organization is at around mid-3 Level in risk management. The assessment underscored some crucial areas for improvement at Level 3, one of the critical ones being the risk manager's lack of involvement in project portfolio risk assessments, highlighting a critical process gap requiring further analysis and alignment.

Apart from the assessment, the participant was tasked with providing additional insights from an organizational standpoint concerning risks and gaps in risk management that impact the project portfolio, seeking suggestions for improvements based on the participant's experience. A query was made whether the risk manager should be more involved in project portfolio risk management.

Other insights and suggestions for improvement made by the risk manager:

According to the participant, the involvement of the risk manager in all projects may not be necessary, but it is crucial for the risk manager to be familiar with the project portfolio's composition. There are instances when a risk manager's involvement is imperative, especially in projects with regulatory or GDPR implications. In such cases, project risks hold significance for the entire organization, as the failure of the project poses a risk of non-compliance.

Furthermore, the organization is currently undergoing a transformative phase, which poses inherent risks from a risk management perspective. The transformation involves changes in human capital, processes, know-how, and organizational structure. Initiation of such substantial organizational changes should ideally commence with a risk assessment session, although it remains unclear whether such a session took place at the insurance company. While not all aspects of the change projects require scrutiny, certain elements should be examined more closely, given their potential significant impact on the organization as a whole. Risk management ought to be considered a fundamental element in this context.

In the context of organizational changes, a shift in mindset is proposed; project managers typically focus on the project management triangle - scope, time, and budget -, neglecting the broader organizational changes, although there should be an emphasis on a comprehensive view of risks arising from sudden organizational changes. In change projects, risks should be viewed via the change itself; evaluating the size of the change, its potential impact and how the change will be managed. Business experts should be involved in the process as project managers often serve as facilitators without in-depth knowledge.

Neglecting the review of risks associated with organizational change will in turn lead to inadequate communication about the change to all employees and missed opportunities to gather valuable information from experts. In the organization, there is an emphasis on the bottom-up approach, leveraging the incident register and engaging with various employees. Risks are identified not by management but by employees, emphasizing the importance of proactive individuals providing warnings in advance. While discussions about risks do not necessarily need to be complex, establishing a routine for addressing them is a healthy practice.

Turning to the company's procedures, the organization has an operational risk appetite statement, but an overarching risk appetite for the company is not defined. This gap requires improvement, especially considering the diverse risks i.e., financial risks, operational risks, ESG risks, risks associated with insurance activities etc. Key Risk Indicators (KRIs) guide risk appetite, but there is room to enhance clarity.

Some operational risks at the company affect projects within the portfolio, one example could be that the same resources are allocated to both project activities and general maintenance, due to which there are constant obscurities whether the projects will be able to meet their deadlines

and deliver the planned scope. Moreover, there is a higher emphasis on (the quantity of) changes with limited time to also ensure their quality. The organization lacks a code freeze, leading to operational challenges during holidays. The absence of intervals for systems stabilization (as it is done in parallel with projects activities) throughout the year poses a risk. Knowing these challenges, it is unclear whether project managers incorporate any time buffers or do contingency planning, highlighting a need for clarity in this aspect.

Following discussions with the risk manager, documents such as the Operational Risk Management Policy, Key Risk Indicators (KRIs), and risk management documents were reviewed. Unfortunately, due to confidentiality reasons, these documents cannot be shared in this study.

4.2. Risk management maturity assessment at project portfolio level

In this section, the risk management maturity specifically within the realm of project portfolio management is explored together with the Head of Strategy and Project Management Division. Like at the organizational level, it was established that the project portfolio had already attained both Level 1 and Level 2 of risk management maturity, therefore, this section provides a deep dive into Level 3 criteria, like in the section above:

Table 8. Strategy and Project Management Division Head's answers in the risk management maturity assessment at project portfolio level

Level 3 - Defined
3.4 Ensure all identified risks have an assigned owner. *"**Yes.** Auditors advised us to include risk owners (and mitigation actions end-date) in our risk and issue register".*
3.6 Identify and record stakeholders' perceptions, considering them in decision-making. *"**Yes/partially,** depending on the project and what stakeholders we have in mind. The perceptions of project owners, project leads, some other key project members are considered in decision-making".*
3.7 Ensure communication and consultation are integral to all risk management activities. *"**Partially**, as we have a risk and issue register where we document relevant risks and issues, which is shown/communicated to the steering board every month.*

However, there is no other routine communication regarding risk management activities. As for consultations, a project manager usually inquires what should be done with certain risks and the risk owners makes the final decision. Unless we think of consultations on a more theoretical level - more like risk management trainings - then these we do not have. Moreover, project managers have weekly meetings where they can discuss risks and issues between themselves, if needed".

3.8 Take account of both the internal and external context when it comes to risk management. *"**Yes,** this is done together with the risk manager. Bigger focus is placed on internal context".*

3.9 Align risk management goals and objectives with organizational objectives. *"**Yes".***

3.10 Systematically find, recognize, record and describe risks. *"**Partially/move towards no**, whilst we do find, recognize, record and describe risks, we do not do that systematically".*

3.11 Determine risk levels and compare them with predefined criteria. *"**Yes**, we do have a matrix with predefined criteria. However, there are no definitions alongside the matrix that is used within the project portfolio and no thresholds either".*

3.12 Prioritize risks for treatment based on strategic considerations. *"**Yes/partially**, as we try to do it and we have the matrix for risk prioritization, however, we look at risks more through their financial impact".*

3.13 Develop a procedure to identify potential positive risks. *"**No**, attention is placed on negative risks, and it is questionable whether trying to identify potential positive risks would bring the company much value at the moment".*

3.14 Identify risks associated with not pursuing opportunities. *"**No**, and it is questionable whether this would be useful at the moment".*

3.15 Study interdependence between different risks and their sources. *"**No,** but it is something that more attention should be given to".*

3.16 Incorporate cost/benefit analysis for each risk treatment option. *"**No**, but when we decide on the mitigation plan for a risk, we decide what is the best course of action, and it would be too time-consuming to start doing cost/benefit analysis for each risk treatment options especially as we have highly limited resources".*

3.17 Identify, communicate, and monitor secondary risks. *"**No**, as the company does not have definitions for secondary risks".*

3.18 Record, monitor and review all risk management activities comprehensively. *"**Partially/move towards no.** There is no comprehensive reporting, but it is also one of the areas that more attention should be given to".*

Source: composed by the author

As per this assessment, it was determined that the project portfolio is around mid-3 Level in risk management, although the portfolio's risk management maturity is below that of the organization's, as the organization currently uses more comprehensive templates for risk activities tracking. The project portfolio is influenced by risk management decisions at the organization, i.e., the absence of procedures to identify positive risks (opportunities) and definitions for secondary risks, coupled with the lack of comprehensive reporting and historical information etc. It is worth to note that whilst exploring positive risks (opportunities) and risks associated with not pursuing opportunities may not seem immediately beneficial, such considerations could enhance long-term strategic planning.

On the other hand, there are a few areas for potential improvement within the portfolio, such as addressing the lack of attention to interdependencies between risks and their sources and the absence of systematic approaches to identifying, recording, and describing risks, for which the project portfolio would need more comprehensive reporting. Additionally, the current emphasis on financial impact in risk prioritization suggests a potential refinement by incorporating broader strategic considerations. There is also room to strengthen stakeholder engagement by consistently considering perceptions of more stakeholders across projects, which would foster a more proactive risk culture. Striving for a shared responsibility in risk management is valuable, fostering a more robust and cohesive risk management culture.

Apart from the maturity level assessment, an additional questionnaire was created to get more context and to look more in-depth into certain areas, such as risk management documents and guidelines, as from the assessment alone the depth of project portfolio risk management is not visible (as some criteria might be met superficially):

Strategy (please briefly comment the following point for context):

- How are strategic opportunities identified and evaluated? *"Project portfolio consists of activities that support the company's strategy. Based on the set financial goals, the management analyzes where we could get more profit from. For example, we identify an opportunity that we could get more profit if we can start selling new products through online brokers and then we start new integrations with them. Although, there is no single definition of how to identify and evaluate strategic opportunities. At the core of strategy, we have financial goals and the strategy must achieve profit (other measures are secondary)".*

Governance:

- Are there specific policies or guidelines that guide risk management within the portfolio governance framework? *"We have Project Management Procedure which contains definitions about: project risk, project risk and issue log, risk management, the responsibilities of each role within projects in regard to risks. The document has a list of inputs and outputs for each project phase, for example, in the planning, one of the inputs is to assess and register possible risks and issues, review/coordinate the assessment with Risk & Compliance, and the output is to update the project risk and issue log. During closure, project risks and issues are closed or moved to business organization. There are no further guidelines on risk management activities".*

Whilst there is a requirement in the guidelines to review/coordinate the risk assessment with Risk & Compliance, it is not clear how this is realized practically (or to what extent), as the risk manager noted that they are not involved in project portfolio risk management activities.

- Are there mechanisms for continuous improvement in portfolio governance practices related to risk management? *"No, but we have audits for project portfolio activities, including its risk management practices. We get comments from auditors*

on what could be improved. However, we are not very proactive ourselves in advancing our risk management framework".

Capacity and Capability Management:

- What are the biggest challenges when it comes to resource allocation within the portfolio/programs? *"Biggest challenge is dependency on a single key resource. In general, resource conflicts are not a bad thing, as having conflicts makes us prioritize tasks better and focus on deliveries that are the most valuable. Although we must know our tolerance level for it".*

Stakeholder Engagement:

- What are the main risks related to stakeholders/stakeholder engagement within the portfolio/programs? *"We used to have issues before, as owners' engagement in projects was low. Owners' responsibilities were changed over time to have them more involved. Currently, the main risk would probably be an overload of owner capacity".*

Expected Value/Benefits Delivery:

- How does the portfolio/programs maximize opportunities to increase value? *"We do not seek new opportunities through the transformation program itself. We do not even try to identify unexpected opportunities. We do what is planned. Although the scope sometimes changes depending on the owners' wishes".*

Portfolio risks management:

- How satisfied are you with the timeliness of reporting on emerging risks by portfolio component leads? *"One thing is the documentation/reporting itself, another is verbal risk escalation. The latter is quite good. However, we need to try to document all those risks that were escalated verbally".*
- Are there established criteria for determining when a risk should be included in the risk register or escalated to higher levels within the organization? *"There are no such criteria".*

- Is there a repository where systematic risks are identified, documented, and reviewed across the entire portfolio or program? *"We have a risk and issue register, but this area could be improved to start recording all risks to be able to identify systematic issues/have historical data, not just about risks and issues, but also about taken mitigation plans"*.
- Can you describe instances where and how lessons learned from past risks were applied to enhance future risk management? *"We used to have lessons learned file with smaller projects, during the transformation program they disappeared because all the projects lasted for a very long time (lessons learned were not updated for about 2 years)"*. However, the participant could not recall if anything was adapted from lessons learned to new projects.

Concluding questions:

- Which specific risk management practices do you think could be strengthened, and what suggestions do you have for improvement? *"It would be great to construct better risk management guidelines if our current procedures are too abstract. Moreover, we need to start reporting risks and issues more comprehensively to have historical data. This way, we will be able to identify systematic issues and have a track of what kind of mitigation actions were taken"*.

Based on the answers from the Head of Strategy and Projects Management Division, it was deemed that the pursuit of Level 4 in risk management maturity may not be prudent, as there remains substantial work to be achieved on Level 3, with each criterion requiring qualitative fulfillment. Given the organization's relatively modest size and constrained resources, a discerning approach is imperative in determining the necessary risk management enhancements. Opting for incremental improvements appears to be a more reasonable decision, allowing a slower yet steady risk management maturity progression, with exact improvement actions documented in the conclusions part of the study.

4.3. Integration of risk management processes in the project portfolio components

4.3.1. Project Managers' Perspectives

Risk-awareness assessment

As project portfolio adapts its risk management framework from the enterprise, project portfolio components draw guidance from the overarching portfolio framework. Therefore, the project portfolio risk management framework should be evaluated considering the angle of its different components. In this section, project leads were first asked how much attention is usually devoted to risk identification and assessment within their components to assess what kind of weight this process has in their day-to-day professional lives. A similar question followed afterwards on how well, in their opinion, the culture of shared responsibility for risk management is established within their projects and whether they have any risk assessment sessions together with their team(s).

PM1

"*It depends on the project. Usually, it is not a deep analysis, however, with less successful projects taken mid-way more attention is given to risk (or issue) identification and assessment to bring the projects back on track. We go through risks and issues every week during 1:1 with each stream leader and all relevant risks are then reported to the project owner".*

PM2

"*In different stages risk identification and assessment comes in different weight, the most important part is the planning stage where more attention is given to possible risks, and then there are regular reviews in the execution stage. Usually, these discussions happen organically with the core project management team, which tends to consist of around 4-5 people (project manager, project owner, at least 2 business responsible people, and IT responsible) on the regular basis every week. We review project risks and issues and reassess them, adjusting the list (in the register).*

Business responsible people have their own discussions with project team and bring risks up in a bottom-up approach. However, with the core management team we discuss the project status overall and we do not have meetings regarding risks and issues only. In the discussions there is a focus on the current situation regarding mostly major deliveries, we do not focus that much on risks related to minor things or talk about what could happen in the future".

PM3

"*Risk of not meeting project targets always drives action plans. Risks are identified and assessed continuously on a weekly basis with the owner of the project and the business responsible person. However, in my project the financial target was set a bit too high from the very beginning as organizational expectations were high and it is already known that we will not be able to achieve it".*

PM4

"*In a written form – not enough, however, it is a constant process to think about events that could have a negative impact. There is a bottom-up approach and experts inform the project manager about possible risks, which are then reported directly to the project owner as we have weekly status-update meeting. However, there are no sessions scheduled specifically for risk identification or assessment".*

Drawing from the participant responses, some project managers highlight a proactive and continuous assessment of risks, others note a more reactive approach, with increased attention during critical project phases. The absence of scheduled sessions specifically for risk assessment in some cases suggests room for improvement in formalizing and standardizing the company's risk management practices. Overall, there is a recognition of the importance of addressing risks, but the extent and regularity of these efforts vary.

To refine the existing processes, the involvement of the risk manager as a facilitator for risk assessment workshops during the project initiation phase could be explored. This approach offers a more comprehensive and broader perspective on potential risks, aligning with the risk manager's emphasis on addressing risks arising from change projects. Alternatively, equipping project leads with a list of risk categories to thoroughly review with their teams could enhance risk awareness and management efforts.

Assessment of risk activities reporting

Moving on to the risk reporting section, project leads were queried about their adherence to proper documentation of the risk and issue register and whether it is clear for them how the risks should be categorized/prioritized based on their impact and probability.

Currently, each project has a separate slide featuring its individual risk and issue register, within the transformation program these registers are stored inside a common report that is sent to the steering board. The current format of the risk and issue register used within the project portfolio is as follows:

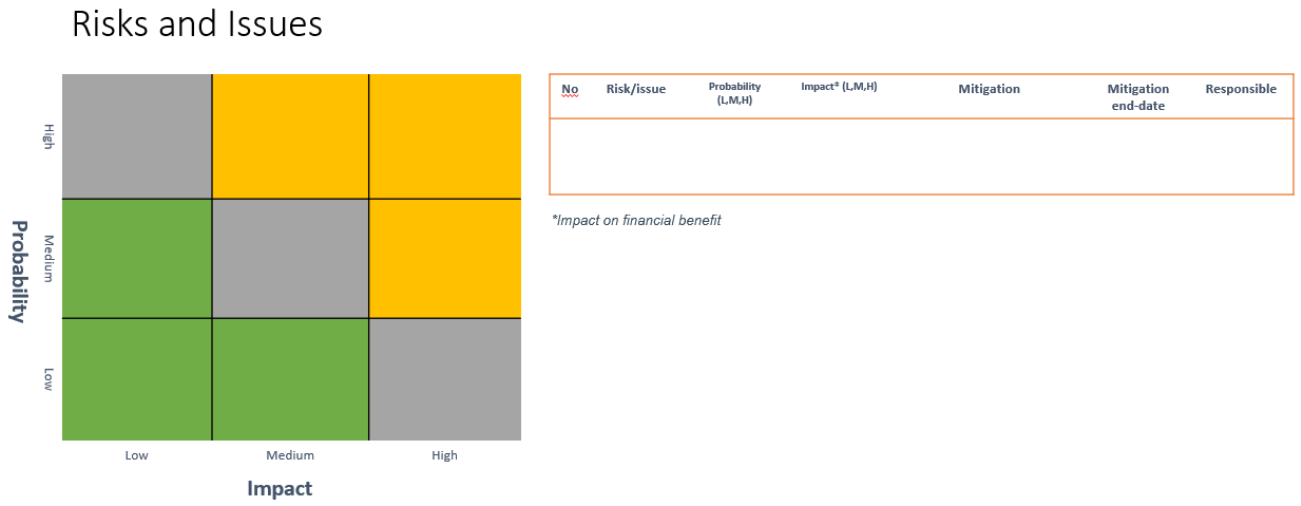

Figure 4. Risk and issue register

Source: material taken from the insurance organization's archives

PM1 indicated that they have "*Very elementary risk documentation and evaluation".* The participant acknowledged that usually the risks' weight is evaluated based on intuition as there are no definitions provided alongside the matrix. When asked if they use any individual file to track risks, the participant replied that they only use the risk and issue register.

PM2

"Yes, but many risks are not documented – we include only major/critical risks. Risks are prioritized based on the yearly business case calculations which is the first point of reference that the team uses as most of the streams and their deliveries generate financial value. We check what was the original idea on how much financial value would be generated and we can then assess that if there is a situation where we will have one month delay, for example, we will lose one month benefit and the exact loss is calculated mathematically".

When asked if more definitions should be provided together with the matrix, the participant responded that it would be useful. Currently, there is a remark in the register that only those risks that have an impact of financial benefit should be reported. However, there are some streams within projects that do not generate financial value but offer other kind of benefits (i.e., customer experience increase, internal process improvement etc.). The participant commented that "*if in the company's strategy we have those other measures/goals, we would also need to somehow involve them in the definitions as well when we report risks. It is a question now that maybe we are not showing risks correctly, and either way there should be no interpretations regarding definitions. It is not entirely clear now whether risks should only be prioritized based on business case calculations or not, as projects get approved that offer other benefits*".

PM3

"*Practically no, just for compliance and presentations. Only those risks are reported that are relevant to the steering board. There are mathematical calculations regarding risk's financial impact*".

PM4

"Only major/critical risks and issues are included in the register and some others are shared with project owner and portfolio manager verbally. We do not use any individual document to track less critical risks within the project itself. At the moment, we prioritize risks intuitively based on what we think has the biggest impact".

Summarizing the responses, it is evident that although there is a risk and issue register, concerns arise regarding the document's depth and comprehensiveness. Project managers often rely on intuition when evaluating risks, tending to focus solely on major or critical risks or issues. Additionally, it was acknowledged that documenting risks is not prioritized. Consequently, the absence of clear definitions on how risks should be prioritized and the reliance on verbal communication indicate areas that require improvement in the company's risk documentation and prioritization processes.

It is crucial to highlight, however, that project managers do actively manage risks, although they are somewhat reluctant to formally document them. Documentation, in most cases, is

perceived as an administrative task post-occurrence. This, however, should not be misconstrued as a lack of risk management by project managers; they do manage risks, albeit primarily verbally.

Dependencies between components

From the risk management perspective, understanding dependencies allows for proactive identification and mitigation of risks. If a project is dependent on another, any delay or issue in the dependent project can impact more than one component within the portfolio. Therefore, project managers were queried about what dependencies their projects have on other projects within the portfolio and how these dependencies are managed, ensuring that they do not become risks. The responses from the four project managers varied in their experiences:

PM1

"*Most of the dependencies are related to IT resources. I used to look through resource conflicts presentations prepared by project managers when we still had those meetings (but in my opinion, they were not successful as we did not manage to agree on priorities). Currently, I just communicate with the team regarding any resource conflicts"*.

PM2

"The main dependency is shared key resources, mostly from IT department. I can find out dependencies and their possible impact on my project(s) through discussions with the key persons in the project, from business and IT responsible persons who manage the resources, backlog and can explain to me the possible impacts, so that I can make necessary communication and prepare responsible persons for decision-making in advance".

PM3

"*Not that many dependencies, it is probably because we do not need IT resources in the project. Some of our deliverables are dependent on other projects, however, they are usually small and we can wait if there are any delays. So far, I have not given much attention to those dependencies*".

PM4

"*The main dependency is key IT resources needed across multiple projects. There are some shared deliveries across projects within the same program (if different parts of the same product*

are being developed in different projects, for example). It happens sometimes that these deliveries come into project's scope mid-year and other things originally approved get postponed. Whilst there is constant communication between project leads regarding any dependencies, we do end up with issues and/or delays, but then it is the management's decision on what should go as a priority".

Insights from the project managers reveal a predominant reliance on shared key IT resources, with varying approaches to managing dependencies. It was mentioned that despite the resource conflict resolution meetings that were carried out at the company, there were continuous challenges with resources. Therefore, the company could benefit from a more refined prioritization mechanism, to have a stronger coordinated approach from the upper management regarding the most important tasks and their delivery schedules across projects.

Resource allocation between components

Consecutively, an inquiry was made about participants' perspective on the sufficiency of resource allocation within the project portfolio components to understand whether each project receives an appropriate allocation of resources. Generally, resource allocation between components is crucial for ensuring optimal performance and meeting predefined goals.

PM1

"*Resources allocation/prioritization is sometimes chaotic, and I think the company does not have enough resources in general, while the management just wants to do more and more. Sometimes I have the feeling that we need clear priorities in the beginning, based on a clear business case. Not to set too many deliveries but instead to prioritize them properly".*

PM2

"*In most of the situations I would agree, except for a few core resources which are required in several projects in parallel and it impacts the performance and deliveries. However, this really depends on what kind of priority the project gets, and it also helps to have experienced project team members who know the processes well and they know how much in advance they need to escalate risks related to resources. I think that is very important, that the team itself does not wait until risks become problems, so that we can reprioritize the tasks in advance".*

Although, in some projects maybe it is the core (the way the scope is planned) that is the problem. Knowing that we have limited resources at the company, we should only prioritize a few deliveries without wanting to do everything in a short period of time. I think it is a good idea to look at the whole portfolio or its transformation program from a wider perspective and try to harmonize deliveries and resource over the main projects. In the planning phase, we should carefully reassess of what could realistically be completed, as another risk out of overplanning could be that the project team(s) would feel constantly demotivated, as despite everything that they achieve they would feel that they are underdelivering".

PM3

"*Resource allocation is adequate, yet it can be improved in terms of division of responsibilities as sometimes it is not clear who is responsible for what exactly*".

PM4

"*It depends on the project, if it is less dependent on internal IT resources – then the allocation is usually fine, and it is then a matter of good planning and communication. If it is an IT-heavy project, resource allocation is not adequate, so there should be a better understanding whether more IT resources should be hired at the company or if we should be less ambitious with our projects".*

The answers suggest a misalignment with internal capabilities leading to ineffective implementation of deliverables within project portfolio components where IT resources are needed, emphasizing the importance of setting realistic expectations and focusing on a select number of high-priority deliverables rather than attempting to accomplish too much in a limited timeframe. A holistic portfolio perspective is useful in this case, considering the collective impact, interdependencies, and strategic alignment of all projects rather than focusing solely on individual efforts in isolation to guide resource allocation decisions.

It was also pointed out that there is a need for improved clarity in terms of the division of responsibilities. This suggests that the governance structure and roles with responsibilities for project members should be reviewed and refined to avoid confusion and enhance accountability.

Risk mitigation

To get more context on what kind of risks there are in project portfolio components and how they are treated, project managers were asked to share an example of successfully mitigated risk(s). Additional question followed on what role does planning a time buffer or creating a contingency plan play in their overall risk mitigation strategy (as the risk manager inquired whether this practice exists within portfolio components):

PM1

"*For example, there was a risk that we might not be able to complete our project's scope with current FTE resources, the risk was escalated to higher management in advance and more people were hired. As for planning a time buffer or contingency planning, I do not have any comments as it seems that it is not a common practice for us".*

PM2

"*Those are very different situations, so one could be – to be able to implement a major delivery on expected timeline, there was a special temporary agreement made with key persons to allocate their time fully on this task and also to work on a few weekends to finalize, and in one situation it was also to postpone vacation plan for a key person. Other example is about detailed planning in advance, discussions about tasks prioritization and dependencies, resource allocation months ahead and comparing with business-as-usual workload and planned vacations, we understood the possible risks of not delivering and with decision makers took an action to work the situation out in the most optimal way.*

Regarding the time buffer and contingency planning, in some situations, we should address more attention to it, but for the key processes, functionalities and systems it is thought off from the initial stage. Also, if it becomes clear that a project is not going to reach its financial target, business responsible do a review of what could be done additionally to bring more financial value. Although, the project manager is not involved in those discussions if no decision is made from the owner's side to include those ideas into the project".

PM3

"*Most of the risks in the project are confidential and cannot be shared, due to the project's nature. Abstractly speaking, there is always a risk that the course of action suggested by the project*

lead and/or the project owner will be disputed by other departments and in this case, either strong arguments must be presented on why that course of action is the best or other ideas must be brainstormed, which I think makes contingency planning integral part of the project? Or at least we can say that we make risk-based decisions all the time, and sometimes these decisions revolve around whether our project's (financial) goals should be pursued. In some cases, even if we know that we may not reach our financial target, identified risks are accepted and a decision is made not to do anything as a different course of action would bring more damage than benefit to the company".

PM4

"As an example, we replanned some tasks to an earlier or later date due to a system's upgrade that was a big blocker for us. I do try to add a time buffer during planning for most deliveries, but I am not sure if this practice is very helpful in most cases as our scope gets changed quite often".

The absence of explicit comments on time buffers or contingency planning suggests a potential area for improvement. Implementing a systematic approach to incorporate time buffers could enhance overall risk mitigation efforts. It is also important to note the comments made regarding confidential risks; as there was a suggestion made by the Head of Strategy and Projects Management Division to refine project portfolio's risk management activities reporting system, additional discussion need to be held whether all risks could be tracked in the same file or report, if some of them are confidential or if it would be just the Head of Strategy and Project Management Division that had access to these files, responsible for keeping a track of historical data.

Risk escalation

To assess if the mechanism for risk escalation is functioning well within the project portfolio, answers were collected whether project managers are satisfied with how leadership is managing and resolving escalated risks. Participants' satisfaction with risk escalation helps disclose several other aspects: if the project portfolio has an effective communication and collaboration process, addressing risks collectively, and if the stakeholders are confident in the company's ability to handle lack of clarity and uncertainties.

PM1

"*With direct manager, yes, but sometimes there is problem to agree between projects, because each project sees their deliveries as a priority and sometimes, we make decisions that are not based on the business case. I think we fail to look at the overall benefit and we lack clear priorities at the company".*

PM2

"*In my projects business responsible key persons and project owners are directly involved and interested in smooth process and on time deliveries, in case of possible risks I do receive the needed support and decisions are taken".*

PM3

"*Mostly, however due to project specifics, some risks that reach leadership are managed as political tools and it is hard to reach an objective decision".*

PM4

"*I am satisfied with how the project owner is dealing with/responding to risks. However, once the risk is escalated and more people (owners of other projects etc.) get involved, it is quite difficult to reach a mutually accepted decision".*

Project managers expressed contentment with project owners, getting the needed support, however, in regard to risks affecting several projects, some dissatisfaction was expressed. A recurring problem mentioned by the participants is the need for clear prioritization and business case alignment, due to continuous challenges to get an agreement between projects as it is not always clear what (which delivery) should go as a priority. This shows the need to implement clearer prioritization mechanisms and aligning decisions with the overall business case, enhancing decision-making.

Current portfolio risk management framework evaluation

Towards the end of the questionnaire, project managers were asked whether the project portfolio has a satisfactory risk management framework:

PM1

"*Medium".*

PM2

"*Initially I did not understand the question. I am not sure what our risk management framework is*".

PM3

"*Formally in a written form no, but practically in a verbal form probably. I would say that it would be good to have a clearer structure/framework for managing risks, but it would bring more administrative work for us".*

PM4

"*I think not, we have quite a basic approach to risk management".*

Insights collected highlight a common need for improvement in the current risk management framework. The consensus indicates an inclination to have greater clarity and structure, emphasizing the importance of a more defined approach. It is apparent that a written, comprehensive framework is lacking, potentially contributing to uncertainties expressed by certain project managers. The call for improvement aligns with the recognition that a clearer, well-structured framework could positively impact the management of risks, even though concerns about increased administrative work were raised as well.

Suggestions for risk management framework improvements

In connection with the question above, suggestions were collected on how project portfolio's risk management framework could be improved:

PM1

"Yes, maybe we can take something from the company's risk management documents. When I look through, there is very good material".

PM2

"*There could be more standard tools (templates) provided to all projects so that this aspect is addressed on an equal basis among the projects. Currently we only have the risk and issue register, but maybe it would be good to instead have individual files to keep a track of less critical risks as well or prepare a risk categories list that could be given to project planning teams at the very beginning or even to new project managers with less experience. However, my idea is that*

these documents should not be mandatory, but instead we should just encourage others to give more attention to risk management in general. If we used individual (confidential) templates, maybe we should also have a broader thinking of what should be included".

PM3

"*Risk management framework can be a bit formalized to find ways of adapting lessons learned practices. Although I have never filled in the lessons learned file myself. Also, maybe we could also think of a better structure for our project leads meetings, so that projects manager could learn from one another?".*

PM4

"*Improve current templates, we could reuse risk management templates that our risk manager uses at the organizational level. At the moment, we do not track systematic risks and we do not see any patterns, so it could be that we are constantly repeating certain mistakes as we keep most of the things in our heads".*

The project managers' suggestions for improving the risk management framework revolve around several key themes. First, there is a consensus on leveraging valuable material from the company's risk management documents. Second, the call for better tools and templates emphasizes that there is an understanding for granularity in risk tracking, while recognizing the importance of flexibility to address varying project needs. Lastly, the emphasis on adapting lessons learned practices and creating opportunities for knowledge exchange through improved project lead meetings reflects a commitment to continuous improvement and shared learning within the company.

4.3.2. Subject-Matter Experts' Perspectives

In this segment, stakeholders with a broader perspective on project portfolio components were subjected to inquiries; these individuals possess a comprehensive understanding of an entire individual program or project scope and/or are preferably involved in multiple components. The decision to conduct this assessment stems from the anticipation that it will help facilitate the identification of systemic risks, contributing to a more thorough examination and understanding of risks that may transcend individual components, and to understand whether these individuals are satisfied with the progress of projects/programs at the company.

Firstly, participants were asked to identify risks or issues that they consider as the main ones (in the projects/programs that they are a part of) which are likely to recur in the future/in new portfolio components:

SME1

"*Clear vision, strategy, goals, priorities, responsibilities, consistency of work and distribution of resources between projects and daily tasks. Measuring the changes made, information storing and sharing".*

SME2

"*Big competition when recruiting for analytical, data science, actuarial, and IT roles; limited substitution of developers; limited number of senior persons in the company with considerable tenure and cross-functional experience. All of these risks might recur next year in multiple projects".*

SME3

"*Lack of resources and lack of communication".*

SME4

"*Based on the projects I've been involved in over the past year, it seems that we have not given sufficient attention to improving our clients' experience. The features that we are developing lack competitiveness in the market, making it challenging to attract a new and younger audience entering the market. We are unable to provide them with an experience that is familiar to them and matches what they find at other insurance companies. From my perspective, it is crucial for us to present a respectable image which we unfortunately fail to do. This is something that will continue into next year".*

SME5

"*Shortage of IT resources and constant resources conflict among strategic initiatives. We plan and prepare project plans, business cases and change requests and only a small part gets implemented".*

SME6

"No knowledge sharing. So, if team members change, it becomes very difficult to work".

In the second question, participants were queried about their satisfaction with the progress of projects/programs within the company and if they believe that the company achieves its goals successfully:

SME1

"*Yes, although not all the planned works were done".*

SME2

"Yes, in the projects that I have been a part of, we achieved huge parts of our most important goals. Though, in some parts we did not tick all the boxes yet, while in other parts we over-achieved".

SME3

"Not satisfied, at the very beginning, when the scope and benefits are prepared, we do not involve the whole team which leads to unrealistic deadlines and targets, therefore, our teams do not believe in projects' goals. We have high ambitions, but we do not have a proper project quality mechanism, therefore, we do not have any definition of what constitutes an unsuccessful project, although there have certainly been such projects. Sometimes we do not even understand what our final goal is as we do not have a good vision. Projects are also intertwined with business-as-usual activities which makes it confusing where the border between project and business-as-usual activities is".

SME4

"*I'm not entirely satisfied with the progress of the projects within the company. While we initially set ambitious goals, many of them were postponed along the way due to lack of clarity and resources necessary for their successful achievement. Although we generated promising ideas and have prepared some for future implementation, uncertainty remains about when we will be able to deliver them to the end user".*

SME5

"*No, as we were able to achieve only ~30 % of what was targeted due to shortage of our own IT resources and our unwillingness to hire external IT resources. If company is struggling*

with cash flows and wants to save on partners and internal IT costs - maybe we can make it clear on the strategic planning and to different activities".

SME6

"*No, as there is a lack of a clear strategy on where we are going as a company in terms of deliverables/features. At the beginning (during initiation phase) it was clear what we had to do, but now everything became unclear and confusing. We have a financial target, but sometimes it seems that the calculation of financial benefits is not accurate, and we fail to deliver many deliverables. Moreover, KPIs from projects are not shared with members who join projects mid-way".*

Stakeholders provide valuable insights into risks and areas for improvement. Responses highlight the necessity for a clearer vision, strategy and revolve around challenges related to resource shortages, recruiting specialized roles, limited cross-functional experience, insufficient attention given to enhancing client experiences, communication gaps and a lack of knowledge sharing. Satisfaction levels with project portfolio components progress vary - whilst some mention achievements, others emphasize delays and concerns related to unclear goals and quality. To navigate these challenges effectively, it is necessary to focus implement improvements that would lead to enhanced strategic decision-making, which is the core for ensuring successful outcomes and foster organizational growth.

CONCLUSIONS AND RECOMMENDATIONS

The theoretical foundation of this study underscores the significance of a holistic approach to risk management that encompasses all facets of an organization's initiatives. This approach enables a comprehensive understanding of the strategic alignment, collective impact and interdependencies between the project portfolio components. As organizations grow, their risk management processes become more defined, standardized, and integrated, leading to progressively higher risk management maturity level.

The identified research gap in project portfolio risk management underscores the necessity for extensive research and practical guidance in the domain of project portfolio risk management. The study is centered around enhancing the maturity of risk management within the project portfolio of the international insurance company, improving decision-making within the company and ensuring that the project portfolio effectively supports the organization’s sustainable growth and success.

The study's hypothesis posits that risk management within the portfolio governance allows a comprehensive approach to effectively manage risks compared to considering them within individual projects. This hypothesis guides the research process, and the research results reveal that the main risk and issues that the company faces currently (e.g., risks related to strategic goals realization, resource dependencies) cannot be adequately addressed through individual projects alone, and it is important to recognize that any gaps within the overarching enterprise risk management framework might have adverse effects on project portfolio components. Therefore, there is a pressing need for a collaborative reassessment and improvement of risk management practices within the organization, emphasizing that project portfolio risk management is not simply a collection of individual projects’ risk management practices.

In the assessment (chapter 4.2.), the maturity level or project portfolio risk management was evaluated at around mid-Level 3 out of 5 levels using the ISO 31000 risk management maturity model. Although, recommendations for improvements focus on incremental progression given the organization's – and the project portfolio’s - size and resource constraints, achieving qualitative fulfillment of Level 3 criteria within the project portfolio risk management before considering progression to Level 4. Nonetheless, the entire section on research results is highly valuable as it contains numerous insights from participants, and all of the collected and analyzed data was

conveyed to the relevant stakeholders at the company who undertake the portfolio risk management improvements.

Recommendations for enhancing project portfolio risk management maturity center around two key areas: processes and human resources management. These critical aspects provide a foundation for the organization to initiate the strengthening of its project portfolio risk management maturity.

Process improvements:

- **Refine the risk matrix**, e.g., by including the definitions alongside the matrix used within the project portfolio for better understanding and consistent application. Existing templates used for organizational risk management can be freely adopted/reused;
- **Consider broadening the criteria for risk prioritization beyond financial impact**, incorporating other strategic considerations. In the templates used by the organization, there are already other criteria provided, which could be reused for the project portfolio. This is relevant if project portfolio components (or individual streams within those components) do not generate financial value but provide other kind of benefits. Currently, there is a lack of clarity on how the financial impact should be calculated, if not all components have a financial target, and if we do not include/prioritize non-financial risks – it raises questions on why the company approves such components;
- **Enhance risk management activities reporting system** to ensure comprehensive historical data storing within the project portfolio, as it facilitates trend analysis, identification of systematic issues and better-informed decision-making, supporting learning and improvement. The existing risk and issue register is adequate, though only a few of the most critical risks deemed significant to the steering board are included there, therefore, the company should consider establishing a risk repository that employs a broader approach. Existing templates used for organizational risk management can be adopted. The confidentiality of some risks should be considered.

  Moreover, the Head of Strategy and Project Management Division should consider implementing a process to analyze the interdependencies between different risks and their sources within the project portfolio. Whilst the organization does not study interdependencies, such an analysis could provide a more nuanced understanding of how

risks interact and impact each other. If it is not enough to just analyze and map documented risks in the register/repository, the company could organize cross-project risk workshops.

- **Reinstate lessons learned integration** as lessons learned from past risks were not consistently applied to enhance future risk management. Learning from past experiences improves risk mitigation strategies and contributes to overall organizational learning.
- **Refine project portfolio risk management guidelines**, currently, the company only has the Project Management Procedure, in which risk management is described in highly generic terms.

  In addition to refining these guidelines, the portfolio should reassess the documentation requirements for its components. The study highlighted certain gaps in the broader field of project portfolio management as well, particularly the lack of quality mechanisms for components within the portfolio. Viewing quality as a risk mitigation strategy, success criteria must be included - quantitative and/or qualitative metrics - in the initial documentation, to measure how well a project performed. Relying solely on financial targets and key performance indicators (KPIs) seems insufficient, and there needs to be a basis for identifying and addressing unsuccessful projects or programs, fostering accountability. A suggested approach would be to do post-implementation reviews and compare the performance of projects against the pre-defined success criteria, however, there should be a formal requirement for this practice within the portfolio.
- **Continue strengthening prioritization mechanisms.** A recurrent issue mentioned by many participants was strategic planning risks - risks associated with how the company formulates and executes its strategic plans. The responses highlighted that the prioritization within the portfolio is unclear and many large components run in parallel, leading to misalignment with i.e., internal capabilities/ineffective implementation.

  One aspect would be to enhance strategic planning, another to periodically maintain and run prioritization sessions with key counterparts with regards to delivery pipeline, third – to review how the organization approaches programs life cycle management, analyzing the sequence on how components within a program should be completed.

  If it is still difficult to set priorities, a suggested approach would be to identify risks with not pursuing opportunities and filter out what would come as a priority and what could be queued.

Human resources management improvements:

- **Engage the risk manager and other stakeholders in proactive risk management framework advancement**. The Head of the Strategy and Project Management Division, serving as the process owner, should initiate communication with the risk manager to address reported gaps in the risk management process and familiarize the risk manager with the components of the project portfolio, to get insights from the risk manager in advance about components' content and possible risks.

  It would be useful to further explore the possibility of involving the risk manager as a facilitator for risk assessment workshops during projects initiation phase, as the risk manager's expertise can provide a broader perspective on potential risks and get more accurate opinion/evaluation from experts. Brainstorming/refinement is needed on (the frequency and format) how the risk manager could be involved in the process.
- **Continuous improvement** (suitable for both areas). If the company wants to continue driving its (project portfolio) risk management maturity upwards, there should be a frequent review of its risk management process, especially as both people and processes change over time, requiring a constant revision of existing risk management practices.

Following these recommendations will foster a culture of proactive risk management, contributing to more successful project portfolio performance and the overall growth of the organization. Some aspects regarding positive risks implementation, definitions for secondary risks etc. were not included in the recommendations, as the changes should first come from the organization's side and then be integrated into the project portfolio.

Study limitations: the study employed a qualitative research method, utilizing a relatively small sample size within a specific company. Consequently, the findings derived cannot be broadly generalized to other companies. Moreover, the results might have been influenced by the researcher's perception, potentially impacting the accuracy and representation of the data.

Proposals for future research: the study could be extended to encompass other industries, thereby broadening the research scope. Employing alternative research methods or expanding the research sample size could offer valuable insights as well.

REFERENCES

1. Andersen, E. S. & Jessen, S. A. (2007). A quick measure of project maturity. Paper presented at PMI® Global Congress 2007—Asia Pacific, Hong Kong, People's Republic of China. Newtown Square, PA: Project Management Institute. Retracted from: A quick measure of project maturity - knowledge attitude and actions (pmi.org)

2. Arlt, M. (2010). Advancing the maturity of project portfolio management through methodology and metrics refinements. School of Property, Construction and Project Management, Design and Social Context. Melbourne: RMIT University. Retrieved from: Advancing the maturity of project portfolio management through methodology and metrics refinements - RMIT University

3. Becker, G. M. (2004). A practical risk management approach. Paper presented at PMI® Global Congress 2004—North America, Anaheim, CA. Newtown Square, PA: Project Management Institute. Retrieved from: https://www.pmi.org/learning/library/practical-risk-management-approach-8248

4. Bissonette, M. M. (2016). *Project Risk management: A Practical Implementation Approach*. Project Management Institute.

5. Fahrenkrog, S. L., Haeck, W., Abrams, F., & Whelbourn, D. (2003). PMI's organizational project management maturity model. Paper presented at PMI® Global Congress 2003—North America, Baltimore, MD. Newtown Square, PA: Project Management Institute. Retracted from: https://www.pmi.org/learning/library/pmi-organizational-maturity-model-7666

6. Faris, R. K. & Patterson, D. (2007). Managing risk in the project portfolio. Paper presented at PMI® Global Congress 2007—North America, Atlanta, GA. Newtown Square, PA: Project Management Institute. Retrieved from: https://www.pmi.org/learning/library/managing-risk-project-portfolio-7297

7. Hartono, B., Wijaya, D. F. N., & Arini, H. M. (2019). The impact of project risk management maturity on performance: Complexity as a moderating variable. *International Journal of Engineering Business Management*, *11*, 184797901985550. Retracted from: https://doi.org/10.1177/1847979019855504

8. Hillson, D. (2012). How much risk is too much risk? Understanding risk appetite. Paper presented at PMI® Global Congress 2012—EMEA, Marsailles, France. Newtown Square, PA: Project Management Institute. Retracted from: https://www.pmi.org/learning/library/2021/06/30/21/03/understanding-risk-appetite-6296

9. Hillson, D., & Murray-Webster, R. (2012). Using risk appetite and risk attitudes to support appropriate risk-taking: a new taxonomy and model. Journal of Project, Program & Portfolio Management Vol 2 No 1 (2011) 29-46. Retrieved from: https://www.researchgate.net/publication/285907050_Using_risk_appetite_and_risk_attitudes_to_support_appropriate_risk-taking_a_new_taxonomy_and_model

10. Hillson, D. (2008). Towards program risk management. Paper presented at PMI® Global Congress 2008—North America, Denver, CO. Newtown Square, PA: Project Management Institute. Retracted from: Towards program Related Risks - Maturity of Project management (pmi.org)

11. Hopkinson, M. (2016). The project risk maturity model. Routledge, London. Retrieved from: https://doi.org/10.4324/9781315237572

12. Iqbal, S. (2005). A unified strategic view of organizational maturity. Paper presented at PMI® Global Congress 2005—EMEA, Edinburgh, Scotland. Newtown Square, PA: Project Management Institute. Retracted from: A unified strategic view of organizational maturity (pmi.org)

13. Institute of Risk Management (IRM). (2018). From the cube to the rainbow double helix: a risk practitioner's guide to the COSO ERM Frameworks. *Institute of Risk Management, London*, 2-21. Retrieved from: irm-report-review-of-the-coso-erm-frameworks-v2.pdf (theirm.org)

14. International Organization for Standardization (ISO). (2009). *ISO/Guide 73:2009, Risk Management — Vocabulary*. Retrieved from: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

15. International Organization for Standardization (ISO). (2004). ISO/ IEC Guide 2 Standardization and related activities General vocabulary (8th ed.).

16. Inclus. (2022). ISO 31000 principles explained – handbook for effective risk management. https://inclus.com/en/solutions/enterprise-risk-management/

17. International Organization for Standardization (ISO). (2018). ISO 31000:2018 Risk management — Guidelines. Technical Committee ISO/TC 262, Switzerland. Retrieved from: https://governance.ie/uploads/files/Internal%20Control/ISO310002018.pdf

18. Jamshidnejad, N. (2021). Selecting the proper model for risk management. *Revista GEINTEC*, 11(4), 210–224. Retracted from: (PDF) Selecting the Proper Model for Risk Management (researchgate.net)

19. Jonas, V. & Chumber, S. (2011). Portfolio risk management: aligning projects with business objectives to deliver value. Paper presented at PMI® Global Congress 2011—EMEA, Dublin, Leinster, Ireland. Newtown Square, PA: Project Management Institute. Retrieved from: https://www.pmi.org/learning/library/portfolio-risk-management-aligning-projects-6194

20. Kashkash, A. (2023). The importance of project portfolio risk management. monday.com Blog. Retrieved from: https://monday.com/blog/work-management/portfolio-risk-management/

21. Killen, C. P., Jugdev, K., Drouin, N., & Petit, Y. (2012). Advancing project and portfolio management research: Applying strategic management theories. *International Journal of Project Management*, *30*(5), 525–538. Retracted from: https://doi.org/10.1016/j.ijproman.2011.12.004

22. Labudovikj, R. P., & Čekerevac, Z. (2014). PROJECT PORTFOLIO MANAGEMENT IN THEORY AND PRACTICE. *MEST Journal*, *2*(2), 192–203. Retracted from: https://doi.org/10.12709/mest.02.02.02.20

23. Lalonde, C. & Boiral, O. (2012). Managing risks through ISO 31000: A critical analysis. Risk Management, 14(4), 272–300. Retracted from: https://doi.org/10.1057/rm.2012.9

24. Lavanya, N. & Malarvizhi, T. (2008). Risk analysis and management: a vital key to effective project management. Paper presented at PMI® Global Congress 2008—Asia Pacific, Sydney, New South Wales, Australia. Newtown Square, PA: Project Management

Institute. Retrieved from: https://www.pmi.org/learning/library/risk-analysis-project-management-7070

25. Martinsuo, M., & Anttila, R. (2022). Practices of strategic alignment in and between innovation project portfolios. Project Leadership and Society, 3, 100066. Retrieved from: https://doi.org/10.1016/j.plas.2022.100066

26. Micán, C., Fernandes, G., & Araújo, M. (2020). Project portfolio risk management: a structured literature review with future directions for research. *International Journal of Information Systems and Project Management*, *8*(3), 67–84. Retracted from: https://doi.org/10.12821/ijispm080304

27. Moeller, R. (2016). Brink's Modern Internal Auditing: a Common Body of Knowledge (8). New York: *John Wiley & Sons*. Retrieved from: https://jabatanfungsionalauditor.files.wordpress.com/2016/06/brinks-modern-internal-auditing-a-common-body-of-knowledge-8th-edition.pdf

28. OECD (2021), Enterprise Risk Management Maturity Model Maturity Model, OECD Tax Administration Maturity Model Series, OECD, Paris. Retrieved from: https://www.oecd.org/tax/forum-on-tax-administration/publications-and-products/enterprise-risk-management-maturity-model.pdf

29. Perera, A. a. S. (2019). Enterprise Risk Management – international standards and frameworks. *International Journal of Scientific and Research Publications*, *9*(7), p9129. Retrieved from: https://doi.org/10.29322/ijsrp.9.07.2019.p9130

30. Pritchard, C. L. (2002). Putting the OUCH in Ouchi! Risk thresholds as a quality and motivational practice. Paper presented at Project Management Institute Annual Seminars & Symposium, San Antonio, TX. Newtown Square, PA: Project Management Institute. Retrieved from: https://www.pmi.org/learning/library/risk-thresholds-quality-motivational-practice-1049

31. Project Management Institute (PMI). (2021). *A Guide to the project management body of knowledge (PMBOK® guide)* (7th ed.). Newtown Square, PA: Project Management Institute.

32. Project Management Institute (PMI). (2017). The Standard for Portfolio Management – Fourth Edition. Newtown Square, PA: Project Management Institute.

33. Project Management Institute (PMI). (2017). The Standard for Program Management – Fourth Edition. Newtown Square, PA: Project Management Institute.

34. Project Management Institute (PMI). (2019). The Standard for Risk Management in Portfolios, Programs, and Projects. Newtown Square, PA: Project Management Institute.

35. Proença, D., Estevens, J., Vieira R., and Borbinha J. (2017). "Risk Management: A Maturity Model Based on ISO 31000," 2017 IEEE 19th Conference on Business Informatics (CBI), Thessaloniki, Greece. Retracted from: (PDF) Risk Management: A Maturity Model Based on ISO 31000 (researchgate.net)

36. Pym, D. V. (1987). Risk Management. PM Network, 1(3), 33–36. Retrieved from: https://www.pmi.org/learning/library/risk-management-9096

37. Rampini, G. H. S., Takia, H., & Berssaneti, F. T. (2019). Critical Success Factors of Risk Management with the Advent of ISO 31000 2018 - Descriptive and Content Analyzes. *Procedia Manufacturing*, *39*, 894–903. Retracted from: https://doi.org/10.1016/j.promfg.2020.01.400

38. Ruslin, Ruslin and Mashuri, Saepudin and Rasak, Muhammad Sarib Abdul and Alhabsyi, Firdiansyah and Syam, Hijrah (2022) Semi-structured Interview: A Methodological Reflection on the Development of a Qualitative Research Instrument in Educational Studies. IOSR Journal of Research & Method in Education (IOSR-JRME), 12 (1). pp. 22-29. Retrieved from: https://www.researchgate.net/publication/358906376_Semi-structured_Interview_A_Methodological_Reflection_on_the_Development_of_a_Qualitative_Research_Instrument_in_Educational_Studies_Ruslin

39. Sanchez, H., Robert, B., Bourgault, M., & Pellerin, R. (2009b). Risk management applied to projects, programs, and portfolios. *International Journal of Managing Projects in Business*, *2*(1), 14–35. Retracted from: https://www.researchgate.net/publication/235280586_Risk_Management_Applied_to_Projects_Programs_and_Portfolios

40. Smith, P.G. and Merritt, G.M. (2002) Proactive Risk Management—Controlling Uncertainty in Product Development. Productivity Press, New York.

41. Teller, J., & Kock, A. (2013). An empirical investigation on how portfolio risk management influences project portfolio success. *International Journal of Project Management*, *31*(6), 817–829. Retracted from: https://doi.org/10.1016/j.ijproman.2012.11.012

42. Teller, J., Kock, A., & Gemünden, H. G. (2014). Risk Management in Project Portfolios is More than Managing Project Risks: A Contingency Perspective on Risk Management. *Project Management Journal*, *45*(4), 67–80. Retracted from: https://doi.org/10.1002/pmj.21431

43. Vargas, D. B., & Campos, L. M. S. (2022). Risk Management: A parallel between ISO 31000 (2018) and the PMBOK Guide (2017). *ResearchGate*. Retracted from: https://www.researchgate.net/publication/373444681_Risk_Management_A_Parallel_Between_ISO_31000_2018_and_the_PMBOK_Guide_2017

44. Weaver, P. (2010). Understanding Programs and Projects—Oh, There's a Difference! Paper presented at PMI® Global Congress 2010—Asia Pacific, Melbourne, Victoria, Australia. Newtown Square, PA: Project Management Institute. Retracted from: Understanding Programs and Projects | PMI

45. Westcott, T. (2005). The risks of risk management. Paper presented at PMI® Global Congress 2005—North America, Toronto, Ontario, Canada. Newtown Square, PA: Project Management Institute. Retrieved from: https://www.pmi.org/learning/library/risks-management-project-life-cycle-7461

46. Zanfelicce, R. L., & Rabechini, R. (2021). The influence of risk management on the project portfolio success – proposal of a risk intensity matrix. Gestão & Produção, 28(2). https://doi.org/10.1590/1806-9649-2020v28e5264