Utilizing Risk Management in Small and Medium-sized Enterprises

Paavo Mattinen

2023 Laurea

Laurea University of Applied Sciences

Utilizing Risk Management in Small and Medium-sized Enterprises

Paavo Mattinen

Safety, Security and Risk Management

Bachelor's Thesis

May, 2023

Laurea University of Applied Sciences **Abstract**
Safety, Security, and Risk Management
Bachelor of Business Administration

Paavo Mattinen
Utilizing Risk Management in Small and Medium-sized Enterprises
Year 2023 Number of pages 29

The goal of this thesis was to identify and assess the maturity of risk management in the client organization and to develop a tangible risk management framework to utilize in the operations. The purpose of the work was to clarify the organization about risk management in general and raise risk management and security awareness within the organization and personnel.

Document review and semi-structured interviews were chosen for the data collection part of the thesis. Document review included some parts of traditional literature review. The process of document review included evaluation and assessment of the documents of the client organization, literature review was implemented as an informal process from basic literature around risk management for enterprises. Semi-structured interviews were executed in the early stages of this thesis and followed a similar framework during the process.

Results from the data collection revealed that the maturity of risk management in the organization were inadequate and required a formalization of a risk management framework to support the organization. The risk management framework constructed is at the basic level and easy to adapt to the operations, the framework walks through a logical path for the author to follow through the risk management process.

It was concluded that this thesis met the requirements set in the early stages and gave the organization a tangible risk management framework to be adapted to the operations and allows developing it according to the needs and decisions made by the organization.

Keywords: risk, risk management, SME

Contents

1 Introduction

In general, risk management has been used in all types of organizations to maximize the potential of business operations, by minimizing threats and maximizing the potential of opportunities. Risk management refers to the coordinated activities to direct and control an organization with regard to the risk (ISO31000 2018, 6).

The goal of this thesis is to focus on assessing and evaluating the maturity of the risk management in client organization, based on the evaluation prioritize risk mitigation and roadmap for delivering risk management plan and framework. The development plan includes a tangible method for the organization to adapt risk management procedures and systems to support their operations and maximize the potential of a growing software development house.

Small and medium sized enterprises (SMEs) in Finland are defined as organizations with lesser than 250 employees and have either an annual turnover not exceeding 50 million EUR or an annual balance-sheet total not exceeding 43 million EUR (Statistic Finland 2022). This thesis discusses the SME's working in the same industry as the client organization is working, and in this regard, the risk management and market environments are evaluated. In addition to the aforementioned definition, The European Commission also includes micro-sized companies under the same acronym, micro-sized companies have less than 10 employees. (European Commission n.d).

Client organization for this thesis is Webso, a software development house based in Otaniemi, Espoo. Webso provides software development solutions and consulting to their clients. Clients are based in wide range of industries, including analytics, logistics, retail and learning environment. The main source of business includes different software development solutions based on the most reliable technologies and architecture varying on the needs of the product, and also consulting to their customers.

In principle, micro, smaller, and medium sized organizations (SME) are not operating as adequate budgets or finances as larger market-listed organizations. It is vital for SME-sized organizations to capitalize their operations as risk free or moderately as possible since the organizations are distinctly dependent on their current and future assets. (Berard & Teyssier 2018, iii) states that SMEs need Risk management much more than large organizations in order to survive.

2 Theoretical background and key concepts

The theoretical background for this thesis is amplified around risk management frameworks allocated towards Enterprise Risk Management (ERM). Main goal of ERM refers to focusing on risks on a strategic perspective by taking the organization in account as a consolidated ensemble. ERM is the process of identifying and addressing methodically the potential events that represent risk to the achievement of strategic objectives and to gain competitive advantage (Chartered Global Management Accountant, 2013).

The key concepts revolve around the topics of risk, and risk management and to their relevance to SMEs and software development houses. Specifically, the thesis explores the importance of adapting effective risk management for the survival and success of SMEs, particularly in the software development houses. The thesis also considers the unique challenges faced by SME's, including financial resources and the rapidly changing working environment.

2.1 Risk as a concept

"Without some understanding of risk and its components, particularly the mathematics behind risk and uncertainty, life today would be a quite different" (Project Management Institute 2017, 453). ERM is not only looking at risks as a negative phenomenon, but it assess the potential of each risk with open communication to investigate the opportunities.

The definition of risk varies depending on the context in which it is being applied to. ISO31000 (2018, 3) provides a definition which states that risk is an effect of uncertainty on objectives, and notes that an effect is a deviation from the expected, it can be positive, negative or both, and can address, create, or result in opportunities and threats. In the field of risk management, the severity of the outcome resulting from the risk is a crucial determinant in assessing and mitigating risk. As viewed through a practical standpoint, identifying, and managing risks is essential for organizations for achieving their goals and maintaining their operations.

A risk is an uncertain event or condition that, if it occurs, will have a negative or positive effect on one or more project objectives (Universiti Teknologi Malaysia, 2007). The concept of risk is multifaceted and context-dependent, with different definitions and implications across various fields of study. The potential outcomes of risk can range from positive to negative, with both opportunities and threats arising from the possibility of an event occurring.

In traditional risk management the risk has been generally viewed as a threat or automatically negatively impacting factor towards the business and its operations. ERM is

neglecting this common understanding of a risk as a concept, the differences between traditional risk management and ERM differ significantly, while traditional risk management usually takes dimensional assessment as a point of view and ERM uses a multi-dimensional point of view in addition to more proactive and continuous mindset while assessing the risks. The COSO ERM, for instance, is using risk appetite and risk attitude in relation to risk portfolio as a tool by assessing the maturity of the organization to take a risk. Positive risk culture is supported if historically grown “risk silos” can be overcome (Hunziker 2021).

2.2 Risk management process

Risk management is a structured approach for the identification, assessment, and prioritization of risks followed by the planning of resources to minimize, monitor, and control the probability and impact of undesirable events (Smith & Merrit, 2002). This definition of risk management summarizes the typical conception from the structures of risk management process. The processes can and are still varying on the details of the context in where the risk management process is being applied to.

Subsequently adapting the typical conception of risk management processes, the typical approach to risk management processes and procedures includes at least following aspects in practice;

1. Risk identification: Involving the identification of potential risks that arise towards the organization.
2. Risk Assessment: Involving the analysis based on the risk identification phase in order to determine the likelihood versus occurrence, potential impact, and risk exposure.
3. Risk Mitigation: Involving the implementation measures to reduce the impacts of identified risks

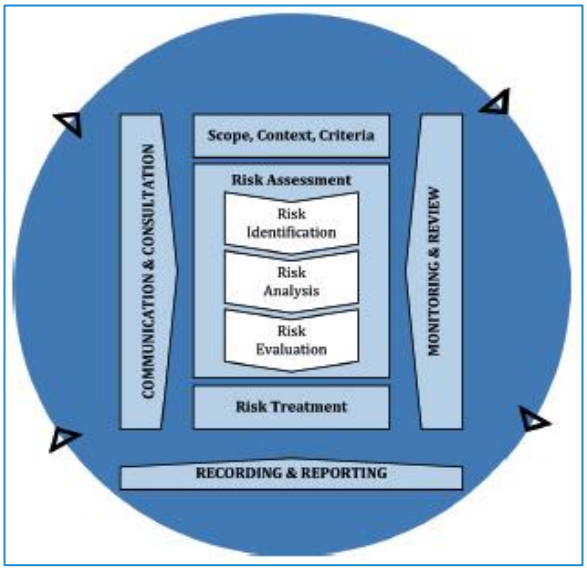

Figure 1: Risk management process (SFS 2018)

As noted by ISO 31000:2018, the risk management process is a tangible framework to be applied to any organization and it gives a moderately free hands for organizations to apply. The process starts with identifying and assessing the scope and the context of the organization, in addition to the environment the business is operating in. The risk assessment phase includes the typical conception of risk management process in addition to risk treatment processes. This is usually viewed as a cycle, where the risks are continuously assessed, treated, reported, and monitored, and the cycle repeats itself.

Figure 2: Risk management process (COSO 2013)

As seen in Figures 1 and 2, the overall entity of the frameworks varies a lot, like the definitions and applicability's of the frameworks. While COSO ERM aims to help organizations understand and prioritize risks and create a strong link between risk, strategy, and how

business performs (Posey, 2021), ISO 31000 is focusing on providing businesses with guidelines and principles for risk management (Posey, 2021). The research executed for this thesis supports combining some aspects from both of the frameworks but still the framework executed for this thesis projects bases its form on the Figure 1.

2.3 Risk management frameworks

Risk theory in general establishes and amplifies a specific framework to contribute into the risk mitigation process. In general risk management theory provides a framework for SMEs to identify, assess and mitigate risks. The most frequently used risk management frameworks for SMEs includes avoidance, mitigation, transfer, and acceptance.

Systematic management of risks relies on literature and frameworks allocated and amplified towards direct environments have been researched and created to serve the needs of the utilizer. In this thesis, the framework's studied are strongly related to ERM modules such as COSO ERM and ISO31000, both aforementioned frameworks provides a guideline adequate to apply in SME sized organization. The differences between COSO ERM and ISO31000 mostly rely on the different approaches between the standards, while COSO is approaching risk management from the financial point of view, the ISO is taking a multidimensional approach everywhere in the organization

One of the key elements while adapting risk management processes into organization's operations is the ability to identify, assess, control, and evolve in the surrounding working and market environment, and to direct the operations systematically towards continuity by understanding completely the organizations elements. ISO 31000 (2018, 10) states that integrating risk management relies on an understanding of organizational structures and context.

In addition to these aforementioned frameworks, different risk management models give the user an excellent tool for organizations to use when adapting the risk management framework. Protection of Assets (POA), Strengths, weaknesses, opportunities, and threats (SWOT), and Hazard & Operability Study (HAZOP) are systematic tools for organizations to utilize especially in while assessing and evaluating operations or direct processes.

2.4 Small and medium-sized enterprises

Small and medium-sized (SME) enterprises are defined by The European Commission as an enterprise that employs less than 250 employees, has an annual turnover of less than 50 million euros and acquires less than 43 million euros in assets. The European Commission also includes micro-sized companies under the same acronym, micro-sized companies have less than 10 employees.

This thesis approaches the acronym according to the definition of The European Commission. Definitions between Statistics Finland and The European Commission are almost identical, but since the organization has not closed an option to work internationally, the acronym used in this thesis is used by the definition of EU.

SMEs in general play a significant part in the economies, especially in Finland where the government and governmental institutions are committed for supporting them. SMEs are if not the most but one of the most important parts for creating job opportunities and thriving for economic growth. By investing in a strong entrepreneurship policy Finland can diversify its business culture and create opportunities for sustainable growth for companies of all sizes (Ministry of Economic Affairs and Employment of Finland, 2022).

2.5 Case company

Webso is a software development house based in Otaniemi, Espoo. Established in 2020 by two computer science students from the University of Helsinki and the University of Jyväskylä. Currently having around 10 employees and advisors around the business. The main business operations are focused on providing different software development solutions and consulting services to clients across a diverse range of industries, including analytics, logistics, retail, and education. Webso has gained a diverse customer base and is experienced in providing software development solutions for various industries and is flexible to adapt and expand the infrastructure and architecture based on the needs of the project.

Webso has proven a successfully ability to adapt to the needs of its customers and the surrounding market environment. At the moment, the company is focused on growing and expanding their business operations. Webso is planning to expand to new industries and technologies and is also working on developing its own online platform.

In addition to the commitment for growth and future expansion, Webso is committed and focused on maintaining and extending a high level of customer satisfaction. The team of software developers and consultants are highly skilled, ambitious, and are keen with high potential in their respective fields, and continuously working to ensure the needs set by their clients. Webso is helping their client organizations and their businesses to achieve their goals and to continuously grow and develop their business.

3 Methodologies

Thesis process started by identifying the research type of the thesis and quickly the decision was made that the research will be executed by utilizing qualitative research methods. Some forms of traditional (narrative) literature review were exploited to support, familiarize, and understand the wider phenomena around the topic researched for the development project. Literature review is a piece of academic writing demonstrating knowledge and understanding of the academic literature on a specific topic placed in context (Institute of Academic Development 2022).

Research executed as explanatory research from the development project for this study. Research on organizations' documents and literature around the studied subject focused primarily on ISO31000 directed towards SME and towards the software development industry, whereas the client organization is also operating.

Research methodologies are supporting qualitative research, document review and semi-structured interviews are commonly recognized as a comprehensive and suitable tool for qualitative research. Using document review and semi-structured interviews as a research methods, it was able to provide a more complete understanding of the organization's operations and practices. The combination of these methods allowed for a comprehensive analysis of the strategies and procedures utilized by the company and helped to identify areas for improvement and further research.

Research methods included document review as a main source of information and semi-structured interview to fulfill the information gaps in the framework. Document review also allocated some aspects from traditional (narrative) literature review to amplify needed information to establish theoretical framework and knowledge base for the study in previous sections of this study.

Both of the selected research methods for this thesis are suitable and used commonly in qualitative research. In general document review involves examining existing documents in order to extract relevant information gathered towards the research questions. On the contrary, semi-structured interviews are generally used by asking open-ended questions to gather data based on respondents' experiences, opinions, and beliefs.

The research methods of document review and semi-structured interviews were chosen for this thesis based on their suitability for the research objectives. Document review was used to identify both the formal and non-formal strategies and procedures that are utilized in the operations of the organization. To fulfill the gaps in the information gathered through document review, semi-structured interviews were conducted. This research method was

aimed at gathering information about the daily activities, practices and procedures employed by the company and its employees.

In research at a general level, validity and reliability are referring as a concepts to evaluate the results of the research in question. As concepts meaning on how well the selected research methods fit and work for the phenomena researched. Reliability is about the consistency of a measure, and validity is about the accuracy of a measure (Middleton, 2019). During the research process the methodologies selected appeared to be easily revealing all the needed data for me to construct the development plan and execute the research. Methodologies were aligned during the whole process of the research and supported the pre-selected methods supporting qualitative research, ultimately the results follow the same path. Meticulous attention to these two aspects can make the difference between good research and bad research (Brink, 1993)

3.1 Document review

To start the thesis process with the client organization Webso, I signed NDA (Non-disclosure agreement) with Webso and the in-depth detail about the internal documentation and contracts will not be revealed in any part of this thesis. During the document review phase, all the internal documentation, procedures, working principles, contracts and basically all written materials were assessed and evaluated. The main idea for the document research was to identify any documentation related to risk management and to familiarize me with the client organization in-depth to base adequate knowledge base needed to continue with the thesis process.

Document review has been generally known as a method that includes analysis of existing documents to gather adequate information from particular entity or phenomena. Even though document review has been especially popular, e.g., in social sciences and political sciences, the research method suits this topic since it discusses particular subjects on wider phenomena and the research methods are executed as a qualitative research. As a research method, document analysis is particularly applicable to qualitative case studies – intensive studies producing rich descriptions of a single phenomenon, event, organization, or program (Yin 2013, 131).

Document review was utilized at the very start of the thesis process to support me in the data collection phase, in order to form a knowledge base for assessing and evaluating the current status of risk management in an organization. The document review is justified to place in order of the research before the following methods since it was chosen to be the main source of information for the data collection. The current state of the document is important for the validity of the information, if the document is outdated and has not been updated or is the

wrong revision of the correct document, this can lead to outdated or inaccurate information on the subject (Bryman 2012, 306-307).

3.1.1 Literature review

Literature review was discovered and utilized in this phase of the research process as a backup methodology to familiarize more in-depth with the literature around the subjects researched. Literature review included an assessment and review of the most essential concepts in risk management literature and was mostly focusing on articles and academics around it. A literature review was not conducted as normative research process, but more as informal implementation and will not be reviewed more in this thesis.

3.2 Semi-structured interview

The semi-structured interview was chosen to be the supportive research method to support and fill the information gaps discovered during the main source of data collection. The structure of the interviews was arranged vary depending on the role of the interviewed person at the client organization. All of the participants for the interviews were working in different roles within the organization and represented different points of views and roles towards the topics discussed during the interviews. This widens the perspective to the data collection to adequately fulfil the information gaps for basing the knowledge base and framework for the development phase of this thesis.

The semi-structured interview method is a qualitative research approach that involves presenting a predetermined set of questions to participants, while also providing the opportunity for open-ended discussion to further explore relevant themes and phenomena related to the research topic. In a semi-structured interview, the researcher has a list of predetermined topics or questions to cover but is also free to explore issues that may arise during the interview (Bryman 2012, 331).

During the interviewing phase of the thesis, the current knowledge base is formed based on the document review, and the interview questions were constructed on the basis of the document review and the previous interviews. The main outlook and framework of the questions were similar, but during and between different interviews the discussion can be directed to different scopes and perspectives needed based on the current knowledge from the researcher. The questions were formed around the following aspects:

1. How is risk management viewed as a concept or method in Webso?
2. How Webso is considering risk management as a part of organizations processes?
3. Why Webso has not included risk management as a continuous process?

4. How Webso would prefer to apply risk management to its operations and processes?

Due to the reason that the interviews were ultimately led to a comprehensive conversation neither than a formal interview, the results are hard to formalize into this thesis report and also due to confidential matters the organization doesn't want to open up the conversations in this report. The results from the conversations about the risk management are encapsulated in the results and development plan of the thesis, where the research problem is been answered.

4 Results

Upon conducting a thorough document review as part of the research process, it was discovered that the case company does not possess any formal written procedures or direct strategies for managing risks, nor does it follow any tangible risk management frameworks. Nonetheless, it was found that the organization does have a well-structured risk assessment procedure in place, which is aimed at identifying and acknowledging potential risks in the environment. By analyzing the documents, this research method was able to provide a comprehensive overview of the organization's practices.

Document review revealed that the organization does not have any current or ongoing procedures regarding risk management. The previously mentioned risk assessment form was discovered but during the semi-structured interview part of this thesis, it was discovered that the organization does not utilize it and some of the interviewed personnel did not know that it even existed. During the semi-structured interview part of the research process, the interviewees were able to provide an overall overview about the organization, their operations, and about the software development industry and working environment the organization is operating in. It is hard for to open up about the results of the interviews in-depth, due to confidential issues.

Taking into consideration the risk assessment form provided from the organization, the knowledge base is based on the provided risk assessment form and can formalize a tangible risk management framework, in addition to the knowledge base acquired from the organization during the document review and semi-structured interviews. The research methodologies supported and provided an adequate overview of the organization and its procedures, on the current knowledge base the organization can be reviewed and the risk management framework can be established to be suitable for the organization.

Furthermore, it should be noted that the absence of formalized risk management procedures and frameworks may leave the organization vulnerable to unforeseen risks and negatively impact its overall business operations. Therefore, it is recommended that the company

consider adopting appropriate risk management practices and implementing formal frameworks to ensure effective identification, assessment, and mitigation of potential risks. This would not only enhance the organization's resilience but also strengthen its competitive position in the market.

5 Development plan

The development plan of this thesis started by defining and investigating the needs of the client organization and by reflecting on the current state of risk management in Webso with ISO31000 and other risk management literature in the field. As implied in the results phase of this thesis, the organizations risk management procedures, guidelines, and methods were at an inadequate level, so fore it is justified to construct a tangible risk management framework for Webso to utilize into their operations. The risk management framework constructed for Webso is amplified to be as simple as possible, in order for the organization to easily adopt it. Only a concrete risk management framework was established for Webso, using, and testing the risk management framework was excluded from this thesis since the thesis agreement and goal of the thesis were to identify and develop the current risk management processes of Webso.

5.1 Goals for the development project

The main goal of this thesis is to provide a tangible risk management procedure for Webso to adapt it to their operations to support business operations and continuity of the organization. The forming of a risk management framework, risk management portfolio to be exact does not include assessing or examining the formed framework. It was excluded from this thesis due to the extent of the portfolio and it does not support the goal of this thesis defined by me or the client organization. Webso's goals for this development plan were to gain a risk management procedures and framework and to develop risk awareness and culture within the organization.

5.2 Evaluation the current state of risk management processes

The evaluation about current state of risk management processes was evaluated during the document review and semi-structured interviews. As mentioned in the previous sections of this thesis, the current state of risk management processes and risk management in general remains inadequate.

To effectively develop the current state of risk management in Webso, an overall evaluation of the organization was needed. In addition to the research methods included in this thesis, it

was justified for the researcher to familiarize also to the working industry and environment, which was the software development industry.

5.3 Framework for risk management system

The goal for the development plan was to create and develop the risk management procedures in Webso by providing a tangible risk management procedure to adapt into their operations to support the business and its continuity, based on the evaluation. The risk management system is explained in this section of the thesis, how is it formed and what circumstances are included in the process of forming the risk management system. The full document from the risk management system presented and explained in the next chapter. The risk management system follows the processes identified and guided by ISO 31000:2018 identifies the risk management process as 5 step process:

1. Identify the risks and the risk categories for each risk
2. Analyze the likelihood and impact of each one
3. Prioritize risks based on business objectives
4. Treat the risk conditions
5. Monitor results and repeat the cycle

The risk management portfolio has been established basing on the knowledge acquired from the research methodologies, familiarizing with the organization and the working environment, and by constructing the risk management framework in accordance with the acknowledged risk management frameworks towards enterprises.

5.3.1 Risk identification process

The process in a risk portfolio starts with risk identification process. The risk identification process will be carried out with a close collaboration with the management of the organization and the employees. Risks will be identified based on risk workshops and discussions around the themes. Utilizing known risk management methods, SWOT-analysis and Bowtie method is justified to use as a tool to help phasing and identifying the risks during the identification process, in addition to this they both support a qualitative research methodology chosen for this thesis.

Even though the Strengths, Weaknesses, Opportunities, Threats analysis (SWOT) main purpose is to act as a strategic planning tool for the organization, it can be utilized also in the risk identification phase in order to identify potential threats by examining the organizations internal weaknesses and external threats posed. By conducting an external analysis, an organization identifies the critical threats and opportunities in its competitive environment (Alrubaiee 2010).

Figure 3: SWOT-Analysis (Wikipedia)

By utilizing the swot analysis in the risk identification process, the organization identifies the internal weaknesses and external threats, by doing this as a risk identification tool forms the knowledge base on the current situation and gives an opportunity to in-depth analyze the threats by using another risk identification tool, in this case bowtie-method.

The Bowtie method is commonly used as a visualization tool for risk assessment that helps to identify the potential threats and hazards posed against the organization the root causes for them to occur. The Bowtie method utilized as a supplementary method to support and fulfill identification aspects in risk management the organization can attain and identify the potential gaps in risk management controls and provide a framework to develop these aspects. The Bowtie analysis is a qualitative risk assessment technology that provides a way to effectively communicate complex risk scenarios in an easy-to-understand graphic format and shows the relationships between the causes of unwanted events and the escalation potential for loss and damage (Lourens & Postma 2018, 1).

Figure 4: Risk Bow-Tie (Talbot 2018)

Even though it has been generally used as an assessment method, this development plan is using risk bowtie method as a supportive tool in risk identification phase, the organization can dig more deeply to the sources and root consequences of each risk, and this method supports and helps also on determining the risk categories, since in this thesis the early categorization of each risk belongs to the risk assessment phase of the process in the following section.

5.3.2 Risk assessment

During the risk assessment phase, it is important to evaluate the significance of the risks and categorize them accordingly. The categorization helps by defining the appropriate actions required in addressing each risk. After the risks have been evaluated and classified into different risk categories based on the risk value and evaluation, it is possible to proceed to the preparation of further action and treatment plans. Taking the aforementioned steps included as a proactive approach to risk management, it is possible to reduce the likelihood of negative outcomes and to protect current assets, reputation, and business continuity.

In the risks assessment phase, when defining the risk values, the framework allocates 5 x 5 risk matrix to be used as a tool to help the user to define the risk value for each risk. The risk matrix is commonly known as a method for defining the level of risk by considering the severity versus likelihood of each risk and the category of such event to occur.

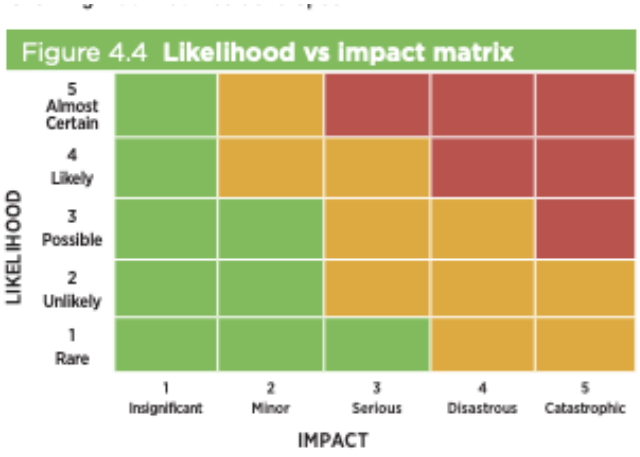

Figure 5: Risk matrix (COSO 2020)

In this framework, there is classified four different risk categories, which includes high, medium, low, and negligible risks. The risks are assessed for each category based on the results of risk evaluation with some help from the risk matrix, in addition to the categorization of each risk, the risks are assessed to three different categories, based on the characterization of each risk. The risk categories chosen for the framework to be applied are; Strategic, operations, and working environment.

5.3.3 Risk treatment

Risk treatment in general has been recognized as a process or component as part of the risk management process. Risk treatment is simply the process of selecting and implementing different measures to influence into the outcome of each risk. ISO 31000 2018 defines the selection of risk treatment options as: Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in relation to the achievement of the objectives against costs, efforts, or disadvantages of implementation.

The risk treatment process usually involves identifying, assessing, and prioritizing each risk, this aims to evaluate and assess the correct influencing method for each risk to minimize the negative effects and to maximize the possible potential effects of the risks. In this thesis the risk treatment processes are based on the following categories:

1. Risk avoidance
2. Risk reduction
3. Risk transfer
4. Risk acceptance

In the following phases of this thesis the aforementioned risk treatment categories are labeled on color formats: basing the order from red to green. The labeling of the categorization of the risks describes the description of each risk treatment method used for each risk based on the individual assessment and evaluation of the risks.

5.3.4 Monitoring and reviewing

Monitoring and reviewing of the established risk management processes is an essential phase of the risk management process. The integration of monitoring and evaluating risk management processes is the key point of development in every aspect of risk management. It gives the key for the author to potentially develop the processes based on the risk management procedures and gives guidelines how to adjust the strategies and risk management procedures used in the risk management process. It’s a continuous process and in this context, it means continuously evaluating and assessing the current and ongoing status of risk management and operations reflecting and developing the risk management decisions made during the processes.

5.4 Applying a risk management system

The section above describes and justifies all of the sections mentioned in the risk management framework constructed for Webso. The framework gives direct guidelines and instructions for Webso and their management to utilize in when adapting risk management to

their day-to-day activities. The following sections describes the risk management charts established for the risk management system and includes justifications.

5.4.1 Risk management process chart

The risk management process chart below expresses the status of previous, executed, or ongoing risk management process. The chart includes the timetable of conducted risk management process, the target evaluated e.g., for a project, the risk matrix used e.g., if the organization wants to utilize a different matrix (not included in the development plan), the participants in the process, identified risk and their descriptions and status part for the risk treatment. Process chart can and is recommended to be utilized in the monitoring and reviewing part of the research process, the risk treatment part for example is easy to monitor throughout the process chart.

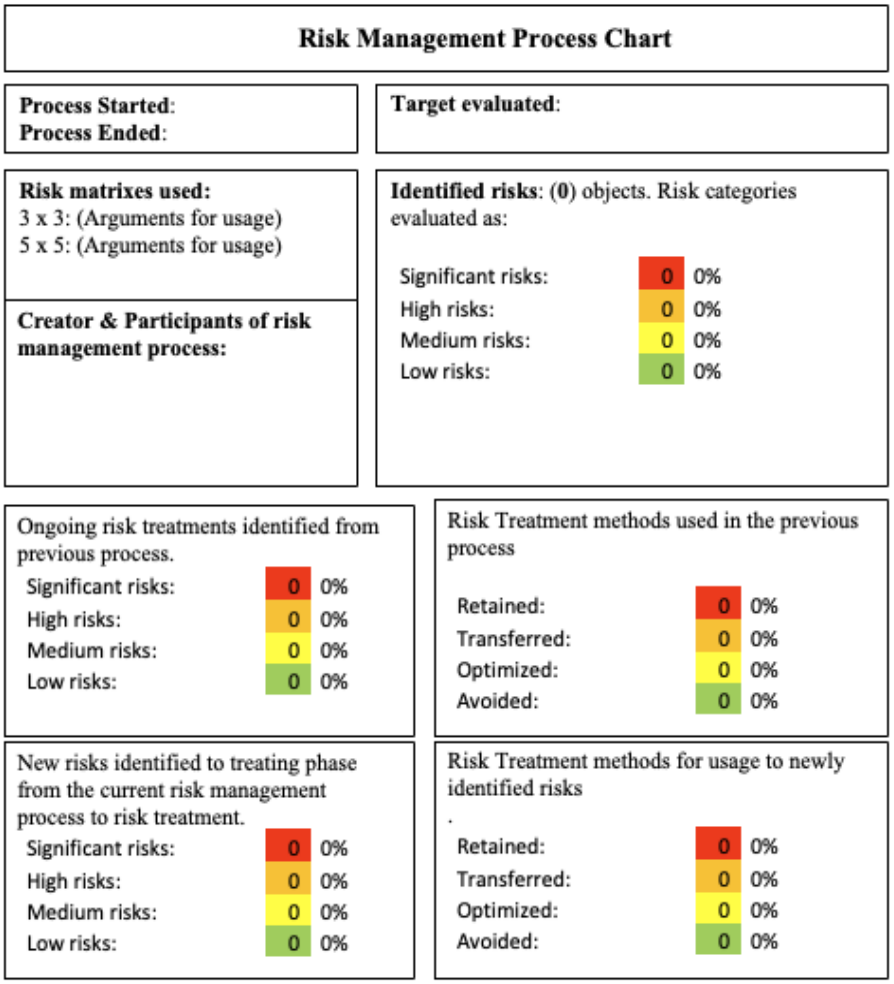

Table 1: Risk management process chart

5.4.2 Risk process list

The risk process list presented below functions as a checklist during the risk management process, where the results can be added when the risk management process is ended. The process list has the name of the identified risk, the risk description, the risk value, and the risk category where the risk has been categorized. This list is planned to be used in the very early stages of the process while the risk identification and assessment part are still ongoing. More detailed version of the process list is presented in the risk assessment form part of this thesis. The definition of these are presented in the sections below. Categorization of each risk helps the creator of the risk management process in the later parts of the process to arrange the risks based on the evaluation aspect of the focus point in the overview of the risk management process.

RISK PROCESS LIST			
RISK	**RISK VALUE**	**RISK CATEGORY**	**RISK DESCRIPTION**
Name of the identified risk	**Score (5)**	Strategic	
Name of the identified risk	**Score (5)**	Business	
Name of the identified risk	**Score (5)**	Operations	

Table 2: Risk process list

5.4.3 Risk identification and assessment process and tools

Charts below represent the identification and assessment tools for risk identification part of the process. Risks will be identified based on the risk workshops and discussions within the organization and the responsible person for the risk management process. The following tools are intended to be used as a supportive tool for the risk identification process, even though either of the tools aren't theoretically towards the risk identification process, they can be utilized in risk identification process and are helping it by the strengths from their purposes. SWOT-analysis can be used to identify threats by analyzing internal and external matters. Bowtie-method can be utilized in the identifying and assessment process to further analyze in-depth the risks and root causes.

STRENGTHS	WEAKNESSES
OPPORTUNITIES	THREATS

Table 3: SWOT-analysis chart

During the discussion in the risk workshop, the user of this risk management framework can utilize SWOT-Analysis as a supportive tool to list the internal and external strengths, weaknesses, opportunities, and threats towards the organization, by doing this the user can have a foresight and opportunities to identify threats posed towards the organization.

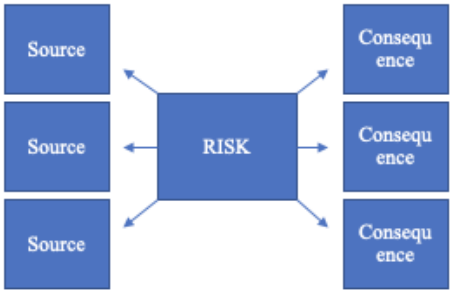

Table 4: Bow-tie analysis chart

Bowtie-analysis as a method for the identification process does not provide just the identification process any tools but can be used as a supportive tool to assess and analyze the risks identified and reasons for the risks, why does it occur, and what kind of consequences the risk could pose towards the organization. This part of the process may reveal new risks or opportunities. It is added in the identification process so the assessing of the risks may start in the very early stages of the risk management process. The risk assessment measures identified can be marked in the risk assessment form expressed in the separate assessment form presented above

Strategic Risk	Operational Risk	Business Risk

Table 5: Risk categories

Risk categories above present the three different risk categories the risks should be categorized. During the process of identifying and assessing the risks in the workshops and utilizing the aforementioned tools. The risks should be categorized in different risk categories which helps the risk management process so fore the risks can be treated accordingly to the processes of the organization

Risk matrix included provides a method for the risk management system to evaluate the significance and risk values for each risk, which provides a quantitative perspective to the risk management process. The calculation of the risk value bases on multiplying the likelihood to consequences, this enables the creator of the risk management process to calculate the risk value and evaluate the risk categories for each risk based on the risk value in their own risk categories mentioned in the risk assessment part of the process and are presented below in this thesis.

LIKELIHOOD						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		CONSEQUENCE				

Table 6: Risk matrix

	Risk value	Magnitude
	16-25	Significant
	11-15	High
	6–10	Medium
	1–5	Low

Table 7: Risk magnitude chart

The risk matrix in the Table 6 represents the calculation method. The visualization for the risk values has also been added to the risk matrix to help the creator to mark and visualize the risks based on the calculation. The magnitudes in the risk value chart represent the risk

categories based on the severity of the risk value, the risk values have been also explained more in-depth in the previous parts of this thesis.

5.4.4 Risk assessment form

The risk assessment form presented below is acting as another checkup tool for the person executing the risk management process. This form should be used after the identification process and assessment processes are done and the author is ready to continue towards the risk treatment process in the ongoing evaluation. In the form the author is able to visualize the name of the risk, the risk value calculated, the risk magnitude calculated by the risk matrix as a color label, and the assessment analyzed and evaluated to be justified for the risk and the risk category on how and why the risk treatment should be done for the risk accordingly. All the texts in the actual form act as an example at this point.

Risk	Value		Assessment	Category
Name of the risk	16		Requires immediate concrete measures	Strategic
Name of the risk	12		Requires clear guidelines for measures and development	Business
Name of the risk	12		Requires clear guidelines for measures and development	Operational
Name of the risk	12		Requires clear guidelines for measures and development	Strategic
Name of the risk	9		Aknowledgement, maintenance and development	Business
Name of the risk	9		Aknowledgement, maintenance and development	Operational
Name of the risk	8		Aknowledgement, maintenance and development	Strategic
Name of the risk	8		Aknowledgement, maintenance and development	Business
Name of the risk	6		Aknowledgement, maintenance and development	Operational
Name of the risk	4		No need for measures	Strategic
Name of the risk	4		No need for measures	Business
Name of the risk	4		No need for measures	Operational
Name of the risk	3		No need for measures	Strategic

Table 8: Risk assessment form

5.4.5 Risk treatment form

Risk treatment form presented below acts as a list for the author of the risk management process to mark the risk treatment processes agreed to be executed for each risk itself. The form color label also expresses the different risk categories in the risk treatment process and are marked in the form at the risk part. This is for the author as a reminder of the change in the color label part.

Risk		Treatment
Retained risk		Requires immediate concrete measures
Transferred risk		Requires concrete measures, clear guidelines for measures and development
Transferred risk		Requires concrete measures, clear guidelines for measures and development
Transferred risk		Requires concrete measures, clear guidelines for measures and development
Optimized risk		Aknowledgement, investigation and development
Optimized risk		Aknowledgement, investigation and development
Optimized risk		Aknowledgement, investigation and development
Optimized risk		Aknowledgement, investigation and development
Optimized risk		Aknowledgement, investigation and development
Avoided risk		No need for measures
Avoided risk		No need for measures
Avoided risk		No need for measures
Avoided risk		No need for measures

Table 9: Risk treatment form

6 Conclusions

Research problem for this thesis was to focus on assessing the maturity of risk management in client organizations and based on the evaluation prioritize risk mitigation and roadmap on delivering risk management plan and framework. Upon conducting the assessment and evaluation the maturity of risk management in Webso, it was found that the organization does not have any formal strategies or basically anything on risk management. During the interviews it was found that the organization was focusing to high growth either than risk analysis and mitigation plans in their business planning and strategy.

During the process of this thesis, after conducting the assessment and evaluation of maturity in risk management and the industry and environment around the organization it was justified to form a roadmap to derive a tangible risk management plan to the organization. The framework was organized to be as simple as possible to lower the ability to utilize risk management as a continuous process.

The risk management framework was formed around the structures from ISO31000 and COSO ERM, including a process chart, identification tools, process list, evaluation chart and treatment form. These aforementioned methods to allocate the formed risk management framework gives tools for Webso to start developing the risk management processes and to adapt them to the operations of the organization.

In a wider perspective, the risk management framework formed for Webso gives the organization the ability to adapt risk management into their operations and develop processes regarding it, for example in project management or consulting perspective. The framework gives basic tools and framework to utilize risk management in a basic level, and opportunity to develop it for more complex usage in the future while the organization has been developing the maturity in risk management and focusing more into it in their strategic decisions.

Reference

Electronic

Alrubaiee, L., Al-Nazer, N. 2010. Strategic planning and performance management: The case of Jordanian mobile phone companies. International Journal of Business and Management. Accessed 30th of April 2023. https://www.researchgate.net/publication/319367788_SWOT_ANALYSIS_A_THEORETICAL_REVIEW

Bérard, C., Teyssier, C. 2018. Risk Management: Lever for SME Development and Stakeholder Value Creation. John Wiley & Sons, Incorporated.

Brink, H.I.L. 1993. Validity and Reliability in Qualitative Research. UNISA. Department of Nursing Science. Accessed 10th of May 2023. https://scholar.google.fi/scholar_url?url=http://curationis.org.za/index.php/curationis/article/download/1396/1350%3Bvalidity&hl=fi&sa=X&ei=MLxaZPDRCYuGmgHX3JsY&scisig=AGlGAw-A7r7N5Ua4PKi-uswGRLxj&oi=scholarr

Chartered Global Management Accountant. 2013. Enterprise Risk Management. Accessed 8 March 2023. https://www.cgma.org/resources/tools/essential-tools/enterpise-risk-management.html

Committee of Sponsoring Organizations of the Treadway Commission. 2020. Compliance Risk Management: Applying the COSO ERM Framework. Accessed 24th of April 2023. https://www.coso.org/Shared%20Documents/Compliance-Risk-Management-Applying-the-COSO-ERM-Framework.pdf

European Commission. n.d. SME Definition. Accessed 9th of April 2023. https://single-market-economy.ec.europa.eu/smes/sme-definition_en

SpringerLink. Hunziker, S. 2021. Enterprise Risk Management. Journal of Business Continuity & Emergency Planning. Accessed 24th of April 2023. https://link.springer.com/chapter/10.1007/978-3-658-33523-6_1

Institute of Academic Development, 2022. Literature review. University of Edinburgh. Accessed 30th of April 2023. https://www.ed.ac.uk/institute-academic-development/study-hub/learning-resources/literature-review

International Organization for Standardization. 2018. SFS-ISO31000:2018. Risk Management. Guidelines. Finnish Standards Association. Accessed 10th of April 2023. https://online.sfs.fi/fi/index/tuotteet/SFS/ISO/ID2/3/648324.html.stx

Lourens, J., Postma, G. 2018. Risk management with Bowtie diagrams. South African Journal of Industrial Engineering. Accessed 30th of April 2023. https://www.researchgate.net/publication/327730575_Risk_management_with_Bowtie_diagrams

Middleton, F. 2019. Reliability vs validity in research. Scribbr. Accessed 10th of May 2023. https://www.scribbr.com/methodology/reliability-vs-validity/

Ministry of Economic Affairs and Employment of Finland. 2022. Government resolution on entrepreneurship strengthens the Governments entrepreneurship strategy. Accessed 10th of April 2023. https://tem.fi/en/entrepreneurship-strategy

Posey, B. 2021. ISO 31000 Risk Management. SearchSecurity, TechTarget. Accessed 27th of April 2023. https://www.techtarget.com/searchsecurity/definition/ISO-31000-Risk-Management

Posey, B. 2021. COSO Framework (Committee of Sponsoring Organizations of the Treadway Commission). SearchCIO, TechTarget. Accessed 27th of April 2023. https://www.techtarget.com/searchcio/definition/COSO-Framework

Project Management Institute. 2017. A Guide to the Project Management Body of Knowledge (PMBOK Guide) 6th Edition. Project Management Institute.

Statistics Finland. n.d. Small and medium size enterprises. Accessed 8th of April 2023. https://www.stat.fi/meta/kas/pienet_ja_keski_en.html

Smith, J., Merrit, D. 2002. Risk Management: An introduction. In J.Smith edition, Risk Management in Business. Routledge.

Talbot. J. 2018. Risk Bow-Tie Method. Accessed 30th of April 2023. https://www.juliantalbot.com/post/risk-bow-tie-method

Universiti Teknologi Malaysia (UTM) 2007. Risk Management Guidelines. Accessed 9th of April 2023. https://www.utm.my/irpa/images/stories/2007/Risk_Management_Guidelines.pdf

Yin, R.K (2013). Case Study Research: Design and Methods. Sage publications.

Figures

Tables