Tomi Ruha

Implementing Risk Management Model in Medium-sized Organization

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Master's Thesis

6 March 2024

PREFACE

At the time of writing this study, this was far too broad an entity at first, and solving this problem took a lot of time and motivation. Initially, the topic was the Cybersecurity management model, but eventually this thesis was condensed into the IT department's Risk Management model, because the previous entity would have been far too extensive. The work was downright painful. The thesis, which was supposed to lighten the Risk Management model, turned out to be more difficult than expected. There are also a lot of things that one found while working on thesis, and many basic things need to be fixed.

Special thanks:
Aicha Löf - who pushed me forward with this thesis.

Erik Klockars - commissioned and my supervisor at work, who had more desire than I did to finish the Thesis.

My kids - who wanted more playing time on the console also said "Dad, could you make thesis so we can play" as well as Seppo Zebra and Kaapo Giraffe (sleep toys).

Ville Jääskeläinen - supervisor of the Thesis, who has given good instructions as the work has progressed and has also been patient when the thesis did not progress at first.

Espoo, 6.3.2024
Tomi Ruha

Abstract

Author:	Tomi Ruha
Title:	Implementing Risk Management Model in Medium Sized Organisation
Number of Pages:	39 pages + 5 appendices
Date:	6 March 2024
Degree:	Master of Engineering
Degree Programme:	Information Technology
Professional Major:	Networking and Services
Supervisors:	Ville Jääskeläinen, Head of Master's program in IT

This thesis was commissioned because the Risk Management Model was not in use in the organization IT department. It was found that what this requires from the organization is a critical entity and that it needs to be investigated. The problem that was solved is dealing with risks in the IT department to avoid bigger problems in the future and to keep critical assets secure. The scope of the work was limited to the operational risks of the IT department and what is needed to get the Risk Management up and running in the organization. This was solved by studying CISSP practices that are linked to the VAHTI Risk Management model, which is based on the ISO31000 Standard. This thesis does not deal with legal or regulatory requirements. This study also excludes Supply Chain Risk Management, project Risk Management and many others such as Threat modeling, even though they also apply to the IT department. This thesis also does not take a stand on quantitative or qualitative Risk Management or the calculation of the monetary value of an asset. One had to draw a line somewhere about what one could include here. The clearest findings are the low level of maturity of the entire organization in Cybersecurity matters, and these issues need to be trained, communicated, and clearly justified. At the end of the day, Risk Management is not just a matter for the IT department, it is an organization-wide issue, although perspectives and risks are different in different departments of the organization. The identification of critical assets and the lack of several policies slows down the implementation of these issues.

Keywords: Risk Management, Risk Assessment, Information Security, CyberSecurity, Risk Identification.

Contents

List of Abbreviations

AAA	Authentication, Authorization and Accounting
AD	Active Directory
AI	Artificial Intelligence
ALE	Annual Loss Expectancy
BC	Business Continuity
CACCA	Cunning Attack Controls Critical Assets
CISO	Chief Information Security Officer
CISSP	Certified information systems security professional
DPIA	Data Protection Impact Assessment
DR	Disaster Recovery
DRP	Disaster Recovery Plan
EDR	Endpoint Detection and Response
EntraID	Formerly Microsoft Azure AD
EOL	End of Life
EPP	Endpoint Protection
GDPR	General Data Protection Regulation
HUMINT	Human Intelligence

IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IR	Incident Response
IRM	Incident Response Manager
ISRM	Information Systems Risk Management
IT	Information Technology
ITSM	IT Service Management
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol over SSL
LDAPS	used denoting LDAP over SSL (LDAPS) and LDAPTLS (STARTTLS) or any other similar secure directory access.
MI	Major Incident
MIM	Major Incident Manager
OS	Operating System
OSINT	Open-Source Intelligence
PDF	Portable Document Format
RACI	Responsible, Accountable, Consulted, Informed
RM	Risk Management

RMB	Risk Management Board
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SIGINT	Signal Intelligence
SLA	Service-Level Agreement
TCO	Total Cost of Ownership
URL	Uniform Resource Locator
VAHTI	The network promotes the cooperation of persons and organizations responsible for the information security of the state administration. The activity is aimed at state administration organizations

1 Introduction

Cybersecurity encompasses safeguarding any entity susceptible to hacking, whether it be a person or a device. It can be broadly categorized into four main areas, as illustrated in Figure 1: Cybersecurity Categories.

Defensive Security: This aspect focuses on safeguarding all assets within an organization's network through the implementation of robust policies and best practices. The primary objective of defensive security is to preemptively thwart unexpected events, such as unauthorized access to the organization's network. Additionally, defensive security involves the detection and response to security incidents. Vital measures, such as regularly updating operating system (OS) versions, patching third-party applications, and ensuring freedom from malware, are integral components of defensive security [1].

Offensive Security: In contrast to defensive security, offensive security involves actively seeking out vulnerabilities in network resources both within and outside the organization's network. This includes practices such as hacking, penetration testing, and exploiting vulnerabilities to gain access to the target's devices and data. The goal of offensive security is to assist the organization in enhancing its defensive capabilities by identifying weaknesses that could be exploited by malicious actors. Additionally, all policies and countermeasures can be rigorously tested in various scenarios as part of offensive security protocols [2].

Network Security: Network security encompasses a wide range of measures aimed at safeguarding network infrastructure. This includes the implementation of virtual private networks (VPN), network segmentation, wireless security protocols, security information and event management (SIEM) systems, firewalls, Intrusion Detection Systems (IDS), and any other components related to network protection. The scope of network security is extensive, covering various aspects crucial for ensuring the integrity and confidentiality of network communications [3].

Social Engineering: Social engineering is a profoundly interpersonal facet of cybersecurity. It involves manipulating individuals to divulge sensitive information or perform actions they would typically avoid, often through deception or psychological manipulation. This can include tactics like phishing emails, pretexting, or baiting. Social engineering encompasses various intelligence-gathering techniques, including Open-Source Intelligence (OSINT), which involves gathering information from publicly available sources. Additionally, Human Intelligence (HUMINT) involves collecting data directly from individuals, such as details about a specific target. Signal Intelligence (SIGINT) involves intercepting and exploiting signals to gather intelligence [4].

While this thesis has delineated cybersecurity into four distinct areas, it is important to acknowledge that these categories often overlap to some extent. The division between them may be somewhat subjective and influenced by individual preferences. Ultimately, the classification of cybersecurity domains can vary depending on the perspective and context of the discussion.

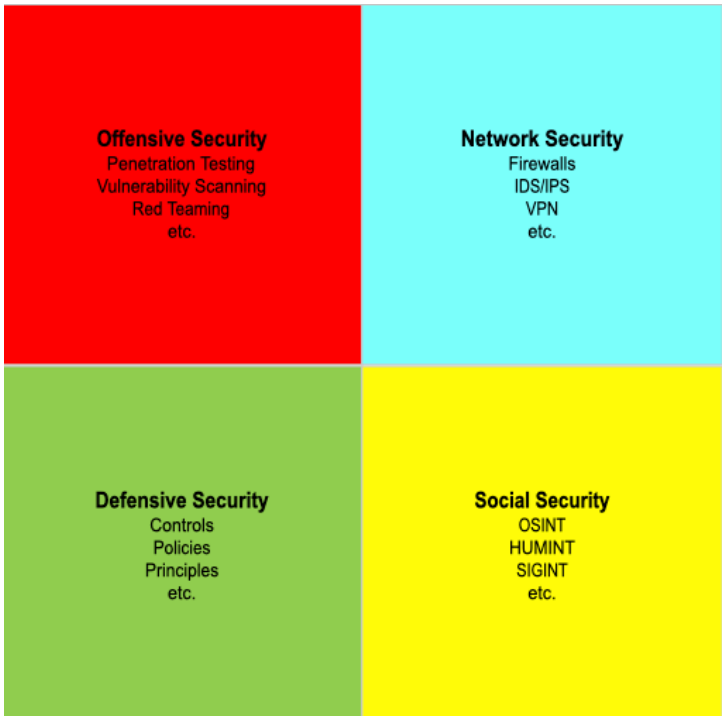


Figure 1: Cybersecurity Categories

Risk Management (RM) constitutes a vital component of defensive cybersecurity, serving to fortify an organization's assets by preemptively preparing for potential adverse events, such as Cunning Attack Controls Critical Assets (CACCA). The primary focus of this thesis centers on resolving issues related to Risk Management and risk assessment within the Information Technology (IT) department. Specifically, this study aims to address the following research questions:

- How to define a light and usable Risk Management process for IT and how to get management support in decision-making, when one does not have any experience on a Risk Management?
- What is needed for the Risk Management process implementation?

Understanding the fundamentals of Risk Management and implementing key processes are crucial for maintaining the sustainability of an organization's IT infrastructure. Risk Management and assessment, though integral to cybersecurity, may often be misunderstood. However, a well-structured and systematic approach to Risk Management empowers managers to make informed decisions that drive better business outcomes.

When assessing risks, it's imperative to also consider potential countermeasures to mitigate undesirable events. In the event of an incident, having comprehensive information and established processes guides the organization towards effective mitigation strategies.

Establishing the fundamentals of Risk Management is paramount before effectively managing risks. This includes gaining a clear understanding of Risk Management and securing sponsorship from senior management. The organization must also identify its assets, particularly business-critical ones, and assign ownership to each asset. For instance, critical business information stored within file systems must be safeguarded to prevent potential disruptions to the organization's operations.

However, garnering support for Risk Management initiatives, amidst various competing priorities, can be challenging. It often requires proactive efforts from

management to champion the cause, rather than expecting initiatives to organically gain traction from bottom-up approaches.

This thesis primarily focuses on medium-sized to smaller organizations, as the client remains unnamed. The objective is to introduce a Risk Management model and emphasize its significance for organizational resilience. The aim is to develop a streamlined operational model, facilitating the initiation of necessary Risk Management processes and enabling future adaptations to meet evolving needs.

The current state of Risk Management within the Organization's IT department is deemed nearly non-existent (refer to Figure 2: Current state of Risk Management). While this presents a concerning reality, it also signifies an opportunity to establish robust Risk Management practices from scratch. Nonetheless, transitioning from conceptualization to practical implementation poses its own set of challenges.

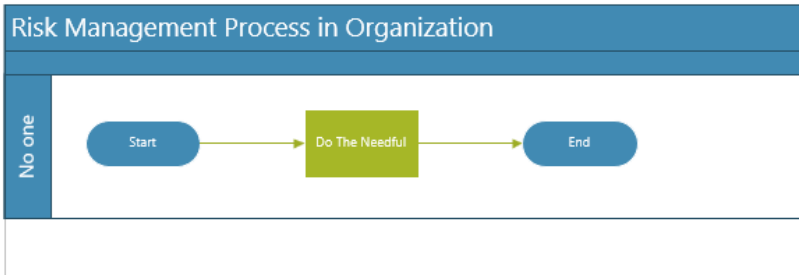


Figure 2: Current State of Risk Management

The absence of Risk Management within the organization's IT department translates to insufficient controls and the presence of unidentified risks within its assets. These undisclosed risks have the potential to precipitate events that could have been averted with the implementation of a robust Risk Management framework.

Risk Management serves as a cornerstone for organizational success, facilitating continuity management and the attainment of set objectives. It should be viewed as a continuous and systematic process that aids decision-making across various

organizational functions and supports organizational development endeavors [5, p 11].

Ideally, Risk Management should seamlessly integrate into management and operational processes, becoming an inherent component of daily workflows. For instance, it should play a pivotal role in change management, procurement activities, and project management initiatives [5, p 11].

The structure of this thesis comprises six chapters, as illustrated in Figure 3: Thesis Chapters. Commencing with this introductory chapter, subsequent chapters delve into specific aspects of the research. Chapter 2 focuses on Research Questions and Methods, while Chapter 3 delves into the Fundamentals of Risk Management, providing a comprehensive overview of its principles. Following this, Chapter 4 explores the Implementation of the Risk Management Process. Chapter 5 presents the proposed solution tailored for the organization, and the final chapter offers concluding remarks.

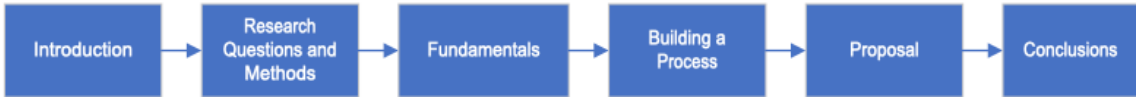


Figure 3: Thesis Chapters

2 Research Plan

This thesis has been commissioned for Organization X's IT department, with the aim of implementing Risk Management practices for future use. Currently, Organization X lacks any form of Risk Management framework, resulting in the absence of controls and related procedures.

2.1 Research Boundaries

The thesis primarily focuses on Information Security Risk Management (ISRM) within the IT Department, referred to as Risk Management (RM). While the study primarily examines information security risks, it does not exclude the exploration of other operational risks within the IT department.

The scope of this thesis is limited to risks specific to the IT department and does not encompass risks related to supply chains, projects, or other organizational areas. Additionally, reputational and budgetary risks, as well as cost-related metrics such as Annual Loss Expectation (ALE), Total Costs (TCO), and Return on Investment (ROI), are not addressed.

The thesis does not advocate for a quantitative or qualitative approach to Risk Management, and it does not delve into the organizational ability to manage risks or seize opportunities. Furthermore, the implementation of the Risk Management model in a production environment is beyond the scope of this thesis.

While the importance of controls in Risk Management is acknowledged, the thesis does not delve into specific control categories but rather presents them at a general level.

Legal and regulatory matters are also outside the thesis's scope. Although they are mentioned at a general level, they are not elaborated on in detail.

2.2 Research Methods

The research methodology draws upon the VAHTI Risk Management Guideline, which is based on the ISO31000 standard, and incorporates perspectives from the Certified Information Systems Security Professional (CISSP) framework and recognized best practices. The VAHTI Risk Management Guide serves as a foundational reference, supplemented and adapted through insights from CISSP principles.

The research initiative commenced upon recognizing the imperative need for Risk Management (RM) within the organization's IT department. The focus shifted towards exploring viable strategies for implementing Risk Management in a cost-effective manner tailored to the context of a medium-sized organization. Additionally, an add-on pertaining to Risk Management was commissioned for integration into the IT Service Management (ITSM) tool, with further design enhancements planned following the initial implementation of core functionalities.

Subsequently, a mind map outlining the Fundamentals of Risk Management was developed to delineate essential prerequisites for initiating the Risk Management model, depicted on the left in blue in Figure 4: Mind map of the Risk Management Research. This served as a foundation for deliberating on the Risk Management process itself, depicted in the upper right corner of the figure. Lastly, considerations were made regarding the implementation phase, with a primary focus on the initial adoption and proper deployment of the Risk Management entity.

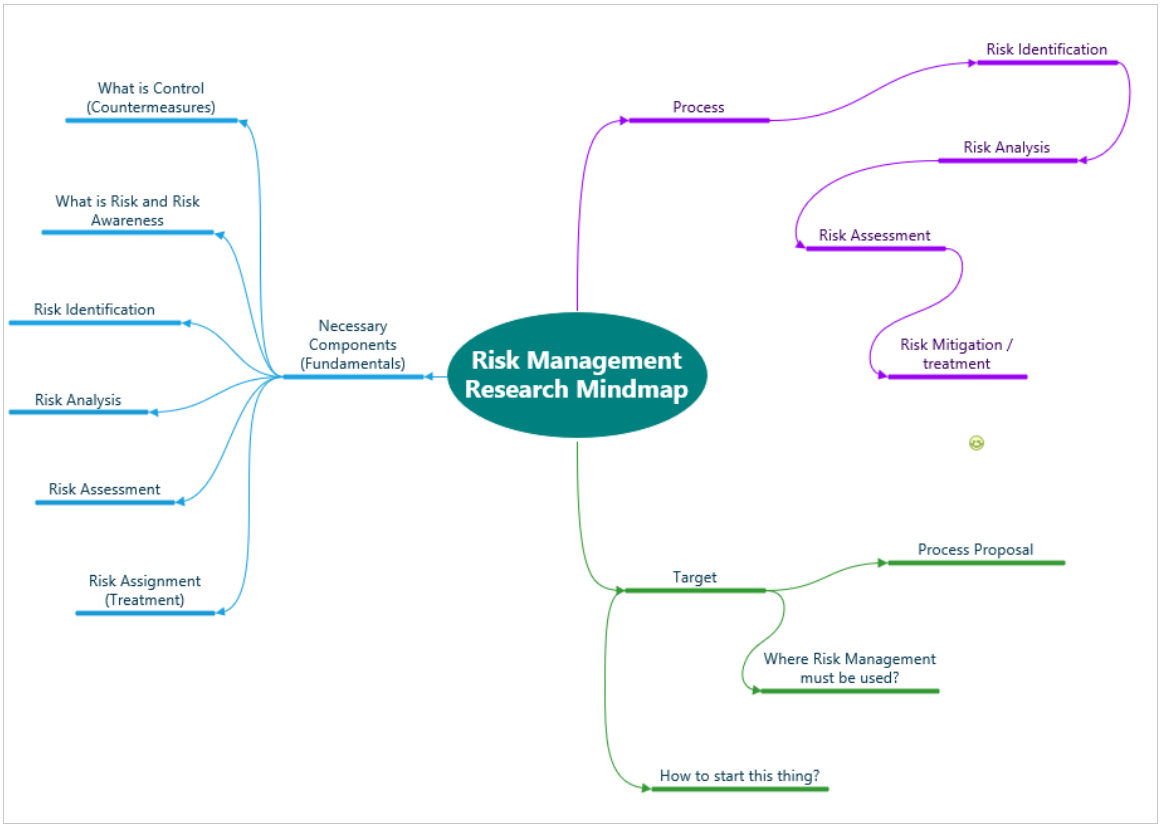


Figure 4: Mind map of the Risk Management Research

This approach allowed us to first identify the fundamental requirements of Risk Management and then outline the procedural steps, leveraging insights from the VAHTI Risk Management Guide and CISSP literature. Drawing upon prior experience, conceptualizing the process proved relatively straightforward. The drafting of the process documentation was also informed by past experiences.

As we approach the pilot phase of the process, the next stage of development entails refining operational procedures and optimizing functionality. This phase will involve fine-tuning operations and integrating the future ITSM system into the process framework.

3 Fundamentals of Risk Management

The cornerstone processes of Cybersecurity and Data Protection are Risk Management and Data Protection Impact Assessment (DPIA). Without a functional Risk Management (RM) framework, organizations risk failing to recognize threats or risks associated with their objectives and may be ill-equipped to respond effectively when unexpected risks escalate. It's important to note that Risk Management encompasses not only mitigating negative outcomes but also identifying potential positive risks or opportunities for the business or its goals [5, p 11-12].

Security-related risk refers to the potential for damage and its consequences if realized. Risk Management involves the systematic identification and assessment of risks, followed by mitigation measures to reduce their impact to an acceptable level, while ensuring they remain at that level. It's essential to acknowledge that not all risks can be entirely eliminated, and achieving complete security is unrealistic [6, p 124].

For Risk Management to effectively support management decisions, it requires an up-to-date understanding of risks and their implications for the organization. Active risk monitoring and clearly defined Risk Management responsibilities are crucial components. Additionally, once a risk has been addressed and assigned a certain status, such as being monitored, it's imperative to revisit it periodically to reassess its impact and adjust measures as necessary [5, p 12].

Even the smallest observation by an individual employee can serve as the starting point for Risk Management, with reporting channels ensuring that relevant risks are escalated appropriately through the established process.

It's essential to recognize that risks, threats, and issues don't disappear simply because they are ignored or deemed unpalatable. Addressing these risks allows managers and organizations to proactively prepare for potential challenges and allocate resources for implementing and maintaining appropriate controls.

3.1 What Is a Risk

A risk is a combination of vulnerability and threat [7, p. 103]. Risks can only be identified and calculated when all three components—asset, threat, and vulnerability—are present [7, p. 103].

The organization possesses critical assets, such as the source code of its software, which pose potential risks. For instance, unauthorized individuals, whether external or internal, gaining access to these assets and potentially stealing the source code constitutes a significant threat. The vulnerability in this scenario lies in the absence of adequate controls to safeguard these assets. Specifically, the organization lacks essential safeguards such as proper accounting and authorization mechanisms, allowing unrestricted access to these business-critical resources. Additionally, the absence of access logging to track activities and identify unauthorized access further exacerbates the vulnerability. Managing this vulnerability is crucial to mitigate the risk of unauthorized access and potential theft of sensitive assets.

3.2 Risk Awareness

While risks cannot be entirely eradicated, organizations must establish the extent of Risk Management and allocate appropriate resources to it. The effectiveness of Risk Management should be evaluated based on the value it adds to the organization. Therefore, it is beneficial to measure the benefits derived from Risk Management initiatives [5, p. 14].

In Figure 5: Risks and Costs, investments in Risk Management are depicted with a red background on the left, indicating minimal or no Risk Management. Conversely, the orange background on the far-right side suggests excessive Risk Management, resulting in higher costs but enabling quicker recovery from potential incidents. This is because risks are likely identified in advance, and controls are implemented to mitigate them.

Finding an optimal price-to-benefit ratio in Risk Management is essential for profitability. Therefore, it is prudent to invest in risks that pose significant threats to finances or reputation. Initiating Risk Management efforts from the yellow area in Figure 5 allows for appropriate investments in the early stages. As the Risk Management model becomes more proficient, adjustments can be made to elevate the level accordingly

Figure 5: Risks and Costs

3.3 Risk Identification

A risk encompasses any undesired event stemming from natural occurrences (such as floods or fires) or human activities (such as viruses, malicious code, or unauthorized access), potentially impacting an organization's assets [7, p. 105].

The primary objective of risk identification is to systematically recognize and document risks and the opportunities they may present. It involves identifying potential sources of risks, events, and changing circumstances that could affect the organization. It's important to note that not all risks are within the organization's control, but they must still be considered, even at a broad level [5, p. 16, 21].

Identifying risks can be challenging, and sometimes it's beneficial to begin with past incidents. By analyzing previous events, valuable experience is gained, allowing for the identification of additional potential risks. For example, the breakdown of a critical server and the subsequent recovery process can provide insights into the potential costs or reputational damage such an incident could inflict upon the organization.

3.4 Risk Analysis

In risk analysis, assessments of impacts and probabilities are interpretive, meaning each participant has their own understanding of the risk and its implications for the organization. Therefore, it is advisable to document these interpretations, ensuring they are realistic and relevant to the specific risk at hand. Ultimately, this information is intended to support decision-making regarding whether a particular course of action is worthwhile.

Risk Management can be approached from either a quality or cost perspective. The cost perspective is typically more straightforward, especially when the value of the asset being protected can be quantified [5, p. 22-23].

Operational risks can be relatively easily estimated numerically by assessing the probability and impact using a predefined scale. Further details on this topic will be discussed in the subsequent section 3.5: Risk Assessment.

3.5 Risk Assessment

The primary objective of risk assessment is to prioritize risks and determine which ones warrant management attention [5, p. 25].

In larger organizations, the number of risks tends to increase, potentially leaving some risks unaddressed. To address this, a common approach is to prioritize risks using the top 10 method, where risks with the highest scores are addressed first. This includes addressing critical and high risks before medium risks. Additionally, decisions must be made regarding which risks are automatically accepted or retired. For instance, risks scoring below eight may be automatically retired. However, it's important not to completely ignore lower risks, as they may still have significance when considered collectively, potentially leading to an accumulation of risk. Workshops can be utilized to address these lower-level risks and possibly identify positive risks.

Risk assessment involves multiplying the likelihood of occurrence by the severity of impact, resulting in a score known as the impact score (see Figure 6: Risk Assessment Matrix.

		Severity				
		1	2	3	4	5
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

Figure 6: Risk Assessment Matrix

3.6 Risk Assignment

A well-executed risk analysis serves as the cornerstone for the subsequent stage of the Risk Management process: risk treatment. Risk treatment involves making decisions regarding how to address identified risks. There are four common risk treatment methods:

- Risk Mitigation: This involves implementing one or more policies, controls, or countermeasures to safeguard assets [7, p. 108].
- Risk Transfer: This entails transferring potential damage associated with the risk to a third party, such as an insurance company [7, p. 108].
- Risk Avoidance: This strategy focuses on completely eliminating the risk by ceasing the activity or condition that gives rise to it [7, p. 108].
- Risk Acceptance: Risk acceptance is chosen when the costs of implementing countermeasures are deemed unreasonable, or when the probability or impact of the risk is low [7, p. 108]

3.7 What is Control

A control is a mechanism designed to safeguard an organization and achieve desired outcomes. Examples of controls include password complexity management and incident response processes. Controls can take various forms,

such as written policies like Risk Management or change management processes. Organizations can implement a wide range of control measures [7, p. 110].

When implementing protections, the balance between security and functionality must be carefully considered. Excessive security measures can impede functionality and hinder productivity. Therefore, it is essential to find a suitable balance to ensure both security and functionality are maintained [6, p. 76-77].

It is advisable for organizations to explore established control frameworks such as ISO 27002, NIST 800-53, or other suitable frameworks tailored to their needs [7, p. 111].

Below are brief introductions to some categories of control types:

- Preventive Controls: These controls aim to prevent errors and unauthorized activities [7, p. 111]. Examples of preventive controls include Risk Management and Change Management.
- Detective Controls: Detective controls are designed to identify errors and unauthorized activities. An example is a video surveillance system [7, p. 111].
- Deterrent Controls: Deterrent controls discourage individuals from engaging in prohibited activities [7, p. 111]. An example is stickers indicating the presence of video surveillance.
- Corrective Controls: These controls are implemented to mitigate the impact of errors and unauthorized events. For instance, restoring system data from backups after a failure [7, p. 111].
- Administrative Controls: Administrative controls encompass policies, standards, guidelines, and best practices [7, p. 111].

3.8 System Owner

The system owner holds the responsibility for overseeing the system's operations. It's possible for one individual to be the owner of multiple systems. Within these systems, data may be owned by various stakeholders. The system owner is accountable for procurement decisions regarding the systems and associated development projects. Moreover, it's the system owner's duty to

ensure that appropriate controls are established to safeguard the system and that comprehensive risk assessments are conducted [6, p. 239].

3.9 Senior Management Support

Effective Risk Management necessitates the commitment of top management towards Risk Management initiatives. This entails having a documented process in place that underpins the organization's operations, such as the Information System Risk Management (ISRM) policy. This policy should align with the responsibilities of the team overseeing the entity. Furthermore, the ISRM policy should be integrated into the organization's overarching Risk Management policy, which forms a part of its information security policies [6, p. 125-126].

For Risk Management to be conducted systematically within an organization, it requires support from senior management and a defined budget allocation. Additionally, there should be a dedicated team responsible for managing risks. In smaller organizations, an individual may take on the role of risk management oversight. It's crucial to recognize that ISRM is just one component of comprehensive Risk Management [6, p. 127].

4 Implementing the Risk Management Process

The aim is to design a comprehensive process accompanied by a sample Risk Analysis and Assessment to illustrate its functionality. This process not only aids in understanding the framework but also serves as a means to evaluate its efficacy. It's imperative to document all actions, even if a risk is retired.

To provide practical insight, a vulnerable web service is utilized as an example, highlighting risks associated with the General Data Protection Regulation (GDPR). The online service's database contains sensitive information such as individuals' names, phone numbers, and addresses. While this case reflects a real-life scenario, additional elements are integrated to enhance the walkthrough's significance. Figure 7: Risk Management Process Preview illustrates, wherein each step is sequentially numbered, and thorough explanations are provided throughout the document. It's imperative to adhere to each step of the process, as skipping any is prohibited.

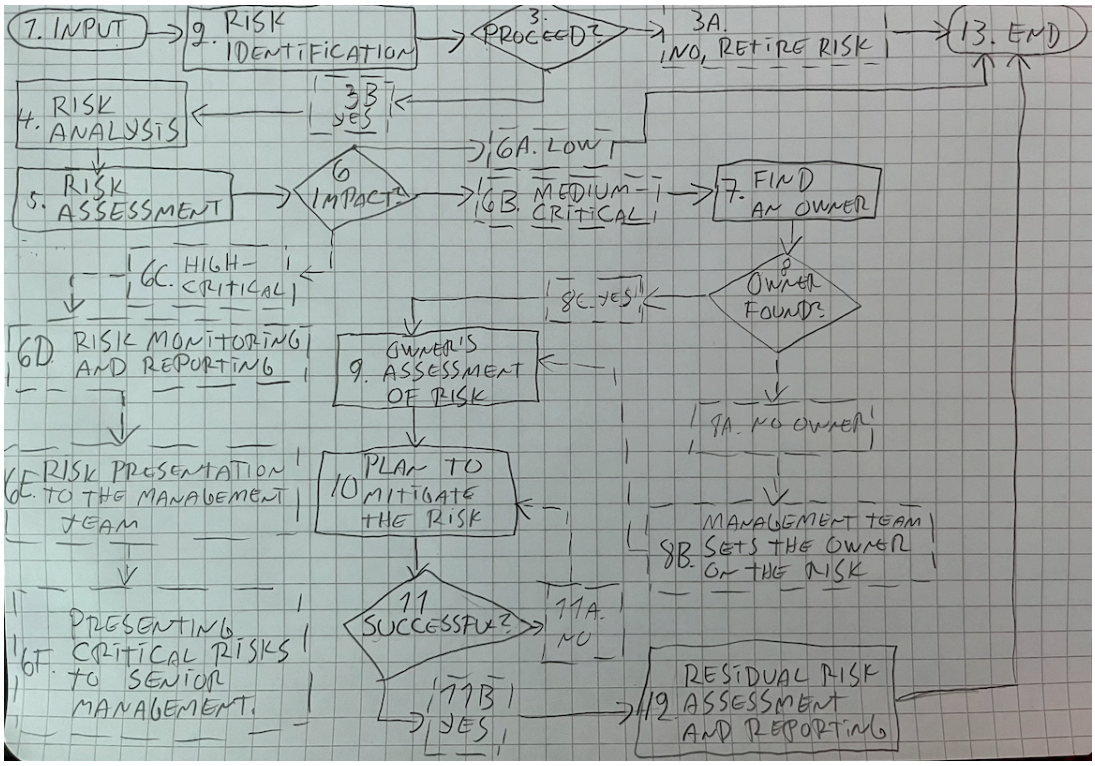


Figure 7: Risk Management Process Preview

4.1 Risk Identification

The Risk Management Process begins with the Risk Input stage, as depicted in Figure 8: Risk Management Process Part 1. Each table within this stage will contain three key components: Action, Information, and Case Path, as illustrated in Table 1: Risk Input.

- Action: This column denotes the process number corresponding to each action.
- Information: This column provides explanatory text to guide the process.
- Case Path: Here, real-life cases that have been previously managed are referenced. Each action is marked with an 'X' to indicate the selected course of action. In cases where multiple actions are applicable, all selected actions are marked accordingly.

This structured approach ensures that each step of the Risk Management Process is clearly defined and that decisions are based on real-world scenarios previously encountered and addressed.

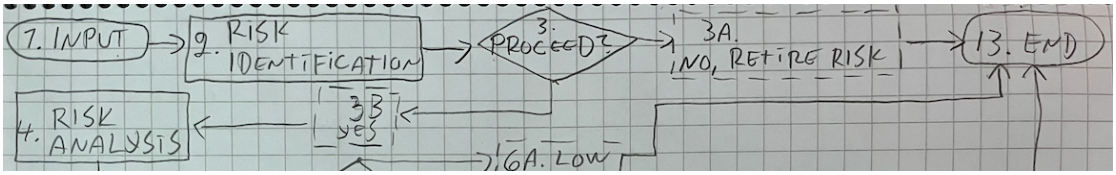


Figure 8: Risk Management Process Part 1

Table 1: Risk Input

Action	Information	Case Path
(1) Input	This input can be any employee by name or anonymous channel or workshop.	x

Case: This is a risk that will cost a lot of money if it triggers an incident; published online service.

Table 2: Risk Identification

Action	Information	Case Path
(2) Risk Identification	Their Risk needs to be Identified as well as Possible by Risk Manager.	x

Case: Risk has been Identified and seems to be valid Risk.

Table 3: Decision 1: Proceed?

Action	Information	Case Path
(3a) Proceed (no) (13) END	if there would be no Risk Identified at this time or does not apply to an organization Risk can be Retired. This would go to (13) END. Must be documented as well.	
(3b) Proceed (yes)	Risk does apply to an organization and worth to be analysed.	x

Case: This needs to be analysed and figured out what to do about it and find ways to mitigate the effects.

4.2 Risk Analysis

It is advisable to establish a Risk Management group to conduct analyses. This phase involves subjective input, allowing all stakeholders to express their views on how risks affect the organization. Sequentially performing risk analysis and assessment is likely the most effective approach to ensure thoroughness. For detailed case analysis, refer to Table 4: Risk Analysis and Table 5: Risk Analysis Breakdown and Figure 8: Risk Management Process Part 1.

Table 4: Risk Analysis

Action	Information	Case Path
(4) Risk Analysis	Members try to come up with possible negative and positive perspectives on risk	x

Case: The analysing team has found the following possible risks. See table 5: Risk Analysis Breakdown.

Table 5: Risk Analysis Breakdown

Analysis	Control needed	Control
All parts are updated in latest patch management?	yes	Currently update process is working, system update order from vendor annually and all critical must be fixed.
There are no MFA available	Yes	Publishing platform which supports MFA and Security Assertion Markup Language (SAML) authentication.
There are no control how Credentials are created and credential are internal	yes	Same as previous. Must request new features from Vendor
Vendor is hard to contact when needed	Yes	Better Service-Level Agreement (SLA) within contract.
This is potential attack surface and can allow unauthorized party to penetrate defences.	Yes	More auditing and alarms on firewall. Publishing platform hides this better. Uniform Resource Locator (URL) sanitation to prevent injections. etc

4.3 Risk Assessment

Risk assessment and impact decisions are crucial components of the Risk Management process (refer to Figure 9: Risk Management Part 2). It is important to determine the severity level and probability of each risk. Additionally, it's essential to recognize that responsibility for managing risks extends beyond the

IT department to asset owners. In fact, Risk Management encompasses various expertise to comprehensively evaluate potential risks. Please refer to Table 6: Risk Assessment for a detailed outline of the assessment process and a real-life case study.

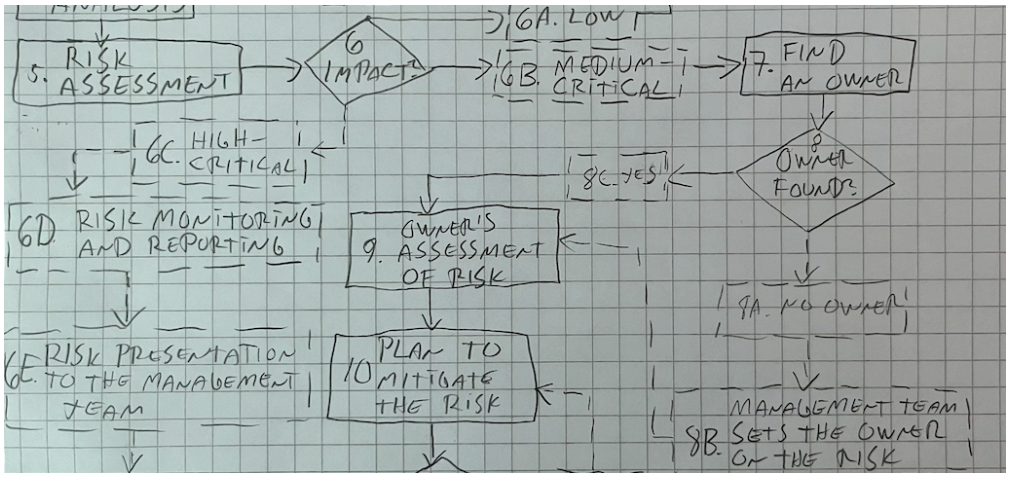


Figure 9: Risk Management Process Part 2

Table 6: Risk Assessment

Action	**Information**	**Case path**
(5) Risk Assessment	Risk Assessment (Likelihood x Severity) Likelihood is set to 4 and severity is set to 5 so score is 20 and it is high Risk and might be critical as well depending on a point of view.	x

Case: In this real-life case, this falls into the red zone (see Figure 10: Case Risk Assessment Matrix) with quite high scores and can be considered highly critical and this risk must be reported to RMB. Risk Assessment matrix (see Figure 8: Case Risk Assessment Matrix) helps to clarify Risk impact to the organization.

		Severity				
		1	2	3	4	5
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

Figure 10: Case Risk Assessment Matrix

To clarify the selection process, the Risk Management Board (RMB) will review items 6c to 6f, and subsequently inform all relevant parties of the progress. For further clarity, please refer to Figure 10: Risk Management 6c-6f.

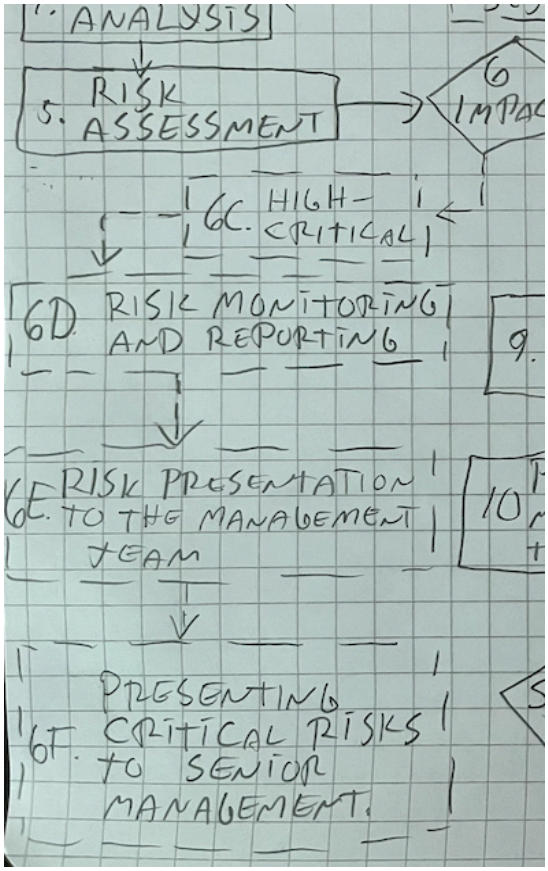


Figure 10: Risk Management 6c -6f

Time for Impact selection (see Table 7: Decision 2, Risk Impact).

Table 7: Decision 2, Risk Impact

Action	**Information**	**Case Path**
(6a) Low Risk impact	Retire and End (13)	
(6b) Medium – Critical risk impact	medium or medium-high; go to step (7) High-Critical steps (6c) and (7)	x
(6c) High-Critical impact	High to critical needs to be reported to Responsible person of Risk Management, should be Risk Management board (6d)	x
(6d) RMB monitors risk and report risk	RMB will monitor and report risk(s) after these Risk are re-evaluated by RMB members and need to figure out if some budget is needed to fix it. (6e)	x
(6e) High-critical impact	Risk(s) reported to the Management team and informed how this is going to be fixed (note: use specialist if necessary) and all possible costs. And what this can cost if not fixed. If critical or decided (6f)	x
(6f) Critical Risk impact	If this is Critical Risk and can impact widely to whole organization and incapacitating big parts of organization or hits to reputation or similar. Then this risk(s) have to report to the Senior Management.	(x)

Case: This case leads to (6b) and (6c). This risk is monitored and reported to RMB (6d). RMB must report this risk to the management team, which decides whether to report this risk to senior management. In this case, the risk should have been reported to senior management, but the problem was that the management team was not interested in this at all. This case failed here. Later,

this discussion group asked for more information as to why this service is not available. Table 8: Find an Owner. to follow this case.

Table 8: Find an Owner

Action	Information	Case Path
(7) Find an Owner	Owner is really needed who can make calls what to do with the system. Owner most likely needs help from IT-team when managing these risks. Incident Response Manager (IRM) or Major Incident Manager (MIM)can make decisions as well if necessary.	x

Case: The owner of the asset was found, and this guy was in a state of panic. So, the IR manager had to decide what to do and removed the publication of the service from the public network. Even if the Owner was found, in each case IRM had to take a risk on its ownership during this case. Table 9: Owner Found? To follow this case.

Table 9: owner found?

Action	Information	Case Path
(8a) No	No owner set, go to (8b)	
(8b) Management team set an owner	Management team finds owner for the system	
(8c) yes	owner found go (9)	x

Case: Owner found. See Table 10: Owner's Assessment of risk to follow case example.

Table 10: Owner´s assessment of risk

Action	Information	Case path
(9) Owner's Assessment of Risk	Owner should use specialist from vendor and from IT-department	x

Case: An update ordered from the supplier to fix vulnerable software components. As already known, AAA (Authentication, Authorization and Accounting) patch was not available. Although many critical issues were fixed, the review score remains the same due to GDPR and DPIA issues. At this point, the published service was removed, but the service remained only in the Local Area Network (LAN).

4.4 Risk Mitigation

Risk mitigation involves the planning and implementation of countermeasures, also known as controls, aimed at reducing risks within the organization. Please refer to Table 11: Plan to Mitigate the Risk, for a detailed plan outlining how these controls will be implemented to mitigate the identified risks, following the example case provided.

Table 11: Plan to Mitigate the Risk

Action	Information	Case Path
(10) Plan to mitigate (reduce) Risk	Plan to and how to mitigate (reduce) Risk. Risk mitigation, Risk Assignment, Risk Avoidance, Risk Acceptance	x

Case: Controls are mandatory here. Risk cannot be avoided or accepted without the consent of senior management and lawyers. The risk cannot be transferred, and the insurance cannot be used.

Risk mitigation is the only viable option. In response, a publishing platform was procured, enabling Multi-Factor Authentication (MFA) through SAML

authentication. However, it's worth noting that the native web hosting service does not support EntraID, Active Directory (AD), Lightweight Directory Access Protocol over SSL (LDAPS), or any other modern and secure authentication methods. Pass-through authentication is also not feasible, resulting in a double login scenario that must be accepted.

For further details on the effectiveness of the mitigation plan, please refer to Table 12: Mitigation Plan Success. Table 12 outlines potential paths, including replanning (11a) and successful mitigation plan execution (11b).

Table 12: Mitigation plan Successful?

Action	**Information**	**Case Path**
(11a) No	Team did not build valid Mitigation plan. Find other specialist if current team cannot Find solution.	
(11b) yes	mitigation actions were successful go to (12)	x

Case: Yes, the mitigation plan was successful and will be implemented. Software update, configuration changes, removal of unnecessary software components, etc. Even if the mitigation plan has been successfully implemented, the residual risk must also be assessed at least annually. see table 13: Residual Risk to follow the case example.

Table 13: Residual Risk

Action	**Information**	**Case Path**
(12) Residual Risk Assessment	There is always residual risk which needs to be assessed and reported. After implementing new controls or alter current controls assessment needs to be redone.	x

Case: The severity remains the same or it can be dropped by one point, now there is more auditing, strong authentication etc and it can be shown that this is properly protected, maybe the severity is now 4. The probability of this incident

can be about 2, a lot of monitoring and this risk assessment inspection annually or if necessary, more often. Our new score is 8 (See Figure 12: Case Residual Risk Assessment).

		Severity				
		1	2	3	4	5
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

Figure 12: Case Residual Risk Assessment

The final step of the process is marked as 13 END. To gain clarity on the various paths leading to the conclusion, please refer to Table 14: End of Process. This table outlines three possible routes to the end, occurring at different stages: at the beginning (3a), in the middle stages (6a), and at the final stage of the process.

Table 14: End of Process

Action	**Information**	**Case Path**
(13) End		x
(3a)	No Actual Risk. Retire and report.	
(6a)	Low Risk. Monitor or retire based on policy.	

Case: The risk has been set to monitored mode and the residual assessment is checked annually. Congratulations, this risk has now been analysed, assessed, mitigated, and set to monitored status.

5 Proposed Solution

Risk Management should be directed towards critical assets within the organization. It's important to note that most organizations already have fundamental controls in place, such as firewalls, backups, user rights management, Endpoint Protection (EPP), and sometimes Endpoint Detection and Response (EDR). Additionally, modern operating systems include embedded software firewalls, and there's often mandatory logging to Security Information and Event Management (SIEM) systems for critical objects. With these basics properly addressed, a significant portion of the organization's assets already enjoys sufficient protection.

Therefore, Risk Management efforts should primarily focus on safeguarding critical assets as per the organization's perspective. Furthermore, Risk Management should also be integrated into projects and changes made to IT services to ensure comprehensive protection and resilience.

5.1 Anonymous Risk reporting channel

An anonymous risk reporting channel provides a beneficial method for employees to report risks within the organization. This approach facilitates the reporting of observations by lowering the threshold for participation. Employees can utilize this channel to report various types of risks, not limited to security or data protection concerns.

Examples of risks that can be reported anonymously or under one's own name include:

- Income leakage Risks
- Budget risks
- General Security risks
- Information security risks
- Data protection risks

- Reputational risks
- Personnel risks
- Damage risks
- Property risks

5.2 Risk Workshops

Risk workshops are organized at least annually and more frequently as required. The primary objective of the annual workshop is to identify new potential risks and evaluate existing risks that have been placed under monitoring. For older risks, an assessment is conducted to determine whether the risk level remains unchanged or has altered due to new risks or threats.

Separate workshops are held for different departments, including the IT department. Identified risks are forwarded to the respective system owner for necessary actions. It's essential to ensure that system owners receive adequate support from the IT department in addressing these risks.

5.3 Where Risk Management should be used

Risk Management should be implemented comprehensively within the organization. However, from the IT department's perspective, it should primarily focus on critical assets. As organizations increasingly adopt public cloud services or Software as a Service (SaaS) solutions, it becomes essential to conduct risk assessments from both security and data protection standpoints. Controls in such scenarios typically involve agreements with service providers, ensuring compliance with data security requirements and legal obligations.

Additionally, integrating Risk Management into projects, particularly during the project initiation phase, allows for the identification of risks from various perspectives such as budget, resource sufficiency, and technology usage. When making changes to the infrastructure, it's crucial to subject them to the Risk Management process to anticipate potential issues. Similarly, assessing risks in

IT procurements involves considering factors like supplier selection, hardware warranties, and Service Level Agreements (SLAs), with warranties and SLAs serving as important controls in this regard

5.4 Risk Management Board

An RMB (Risk Management Board) should be established to serve as the primary Risk Management team responsible for addressing high-level risks across the organization. The members of this board should consist of experts from various fields who can provide valuable insights and expertise. The RMB's role involves managing risks effectively and seeking support from subject matter experts and system owners to ensure that high-level risks are addressed appropriately.

In smaller organizations, the Risk manager may handle this function alone. However, in larger organizations like the target organization, this may not be feasible, particularly for non-IT risks. Therefore, establishing an RMB becomes essential to effectively manage risks across different areas of the organization.

5.5 Ownership

The responsibilities of system owners within the organization need to be clearly defined to ensure consistency and alignment across different teams. Without clear delineation, there may be varied interpretations of these responsibilities, leading to confusion and inefficiencies. It's important to note that the system owner may not always possess technical expertise, thus requiring support from the organization's IT team and potentially from external suppliers, particularly during the planning and implementation phases of risk mitigation strategies. Clarifying these responsibilities helps ensure that all parties understand their roles and collaborate effectively to address risks associated with the systems they oversee.

5.6 Responsible Table

The responsible table should clearly outline responsibilities using a RACI (Responsible, Accountable, Consulted, Informed) framework. This framework effectively designates individuals or roles responsible (R) for specific areas, identifies the accountable (A) party, typically the business owner, outlines who should be consulted (C) for input, and specifies who needs to be informed (I) in case of issues. This labeling system ensures clarity and accountability in decision-making and communication processes within the organization.

5.7 Critical Assets

One of the challenges faced by the target organization is the lack of awareness regarding its critical assets. This lack of clarity makes it difficult to manage assets effectively, whether it pertains to Risk Management, asset management, life cycle management, or any other related processes. While the IT department may have insights into the systems it owns, there remains a gap in understanding what constitutes a critical asset from the perspective of other departments. Additionally, there may be ambiguity regarding the purpose or utilization of these assets across different departments within the organization.

5.8 Proposed Process

The process has been enhanced with the integration of a suitable tool, and to provide further clarity, a swimlane diagram has been incorporated. This diagram illustrates the division of responsibilities among different stakeholders involved in each stage of the process. For a visual representation, please refer to Figure 13: Proposed Risk Management Process.

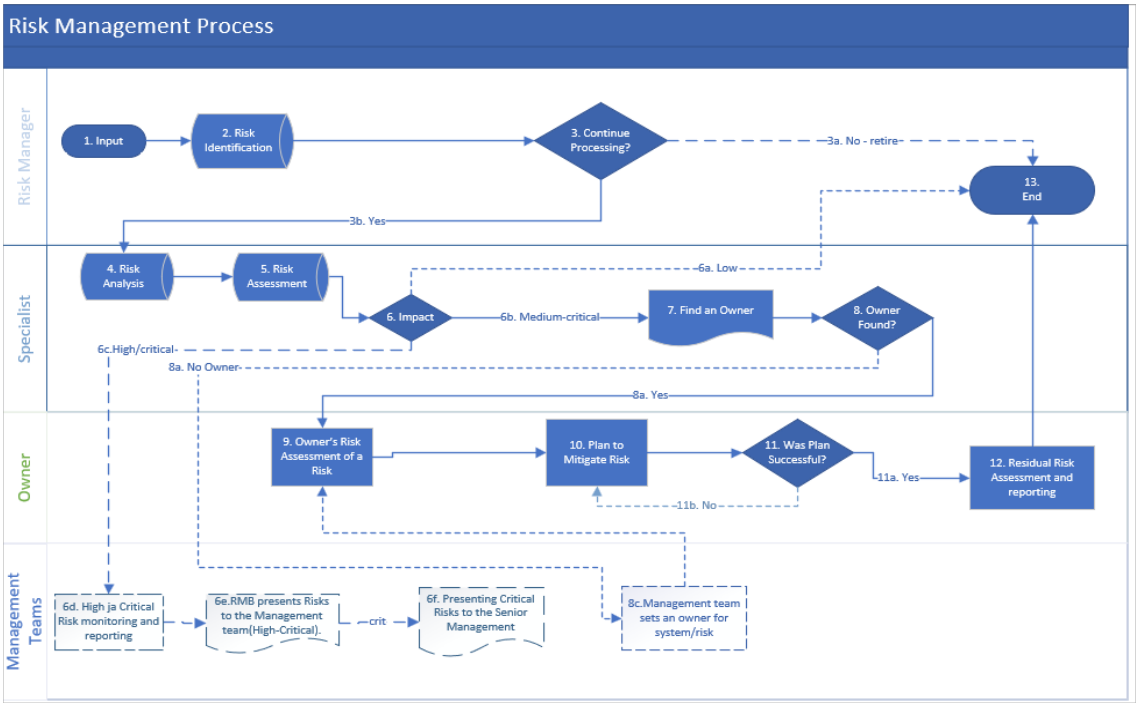


Figure 13: Proposed Risk Management Process

The Risk Manager's role extends beyond being solely responsible for (1) Input; risks may originate from various sources such as an anonymous channel, workshops, or other channels (refer to Figure 14: Risk Manager Swimlane). The Risk Manager holds overall responsibility for managing risks within the IT department and provides support for Risk Management across other departments in collaboration with IT. In addition to facilitating the initial identification of risks, the Risk Manager may also conduct pre-assessments as part of their duties.

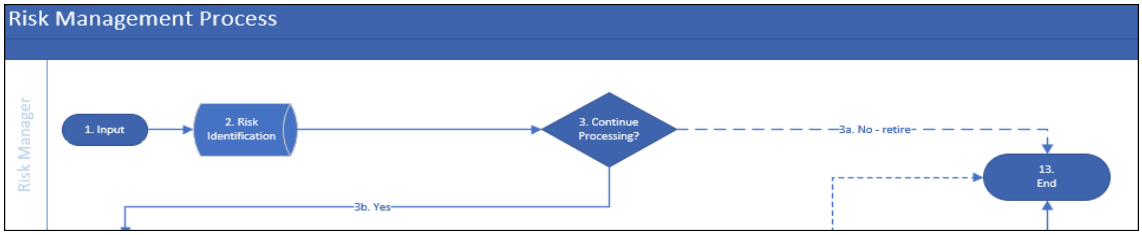


Figure 14: Risk Manager Swimlane

The Specialist, as depicted in Figure 15: Specialist Swimlane, is responsible for conducting Risk Analysis and impact assessment within their designated area of

expertise. This individual may be a member of the ISRM team or an employee of the organization's IT department.

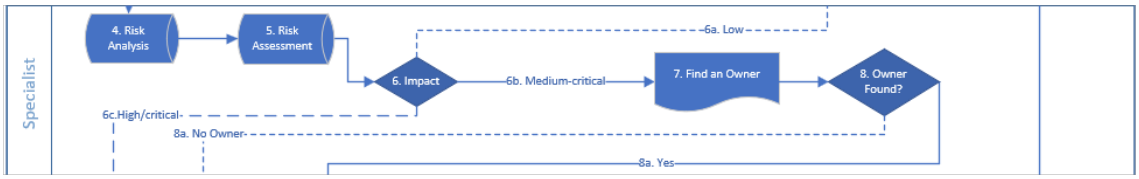


Figure 15: Specialist Swimlane

It is the responsibility of the system owner to conduct their own Risk assessment with the assistance of specialists, as needed. Risk mitigation efforts will likely involve specialists from both the supplier and the in-house IT department. This same group remains accountable for evaluating residual risk, as illustrated in Figure 16: Owner Swimlane.

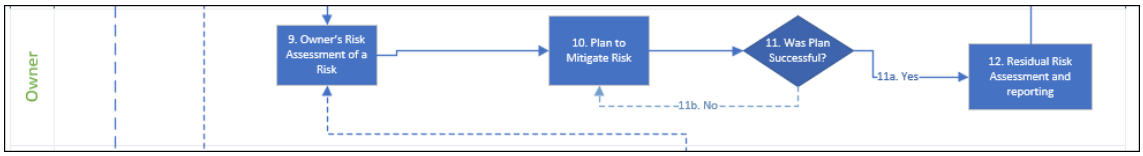


Figure 16: owner swimlane

The RMB serves as a high-level Risk Management Team tasked with raising awareness among the organization's management regarding risks that have the potential to quickly escalate into incidents if left unaddressed (See Figure 17: Management Teams Swimlane). These controls may necessitate funding, prompting the request for emergency budget allocation to mitigate the risks effectively. Moreover, critical risks must be promptly communicated to senior management for their attention and appropriate action.

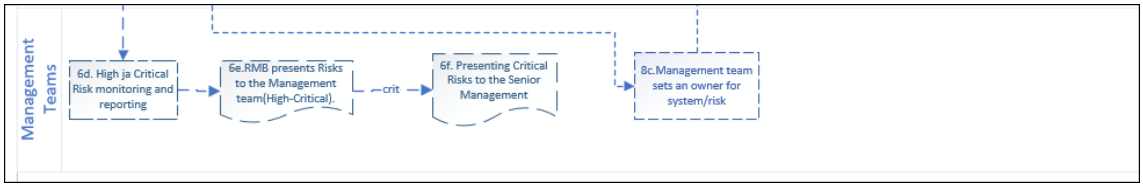


Figure 17: Management teams Swimlane

6 Conclusions

As this thesis approaches its conclusion, the process is poised for piloting. In this final chapter, we will broadly discuss the next steps and critical areas requiring attention to elevate Cybersecurity to an appropriate maturity level within the organization. This is not an exhaustive list of necessary measures, but rather a highlighting of important areas that warrant consideration.

6.1 Research Result

The question now arises: was this Risk Management Model genuinely lightweight? Risk Management is somewhat simplified for IT and Owners through the initial pre-assessment of risks. Further streamlining can occur when risk pre-identification and pre-assessment are partially or fully automated. However, this task requires expertise and keen discernment to ensure that genuine risks are not overlooked due to misunderstanding.

To enhance the effectiveness of Risk Management in IT, one approach is to accept risks with an impact below medium, meaning they are not actively managed because they are deemed unlikely or of low severity. Additionally, implementing a Risk Management tool to aid in managing risks becomes essential. By assigning Risk Management responsibilities to system owners, the burden on the IT department is reduced, transitioning it to more of an advisory role. To facilitate this transition, individuals must be designated as responsible for Information Security Risk Management (ISRM) and general Risk Management, such as the Chief Information Security Officer (CISO) or Chief Risk Officer. With a proven Risk Management Model in place, involving IT personnel in Risk Identification and Assessment can further refine the process through valuable feedback.

In any case, the outcome of the thesis is satisfactory, even if the process was not made as lightweight as originally intended. Now, there exists a process that

requires further development. The deployment of the Risk Management model was beyond the scope of this thesis.

The process becomes somewhat lighter, especially for the owners and potentially for IT, if a Risk Manager preprocesses the risks and evaluates whether they are genuinely significant from the organization's perspective. Refer to Figure 18: Research Result, where the activities of each process step are depicted under the boxes with dotted lines. In the Identification phase, a pre-analysis and possibly a pre-assessment of the risk are conducted. If it is determined at this initial stage that the risk is not significant or genuinely considerable, then the risk is set to a retired state. However, the risk must remain in the system to indicate that it will be addressed if a similar issue arises later.

In the subsequent Analysis and Assessment phase, a similar approach is taken, where IT evaluates whether the risk is as high as initially estimated and whether any existing controls affect it.

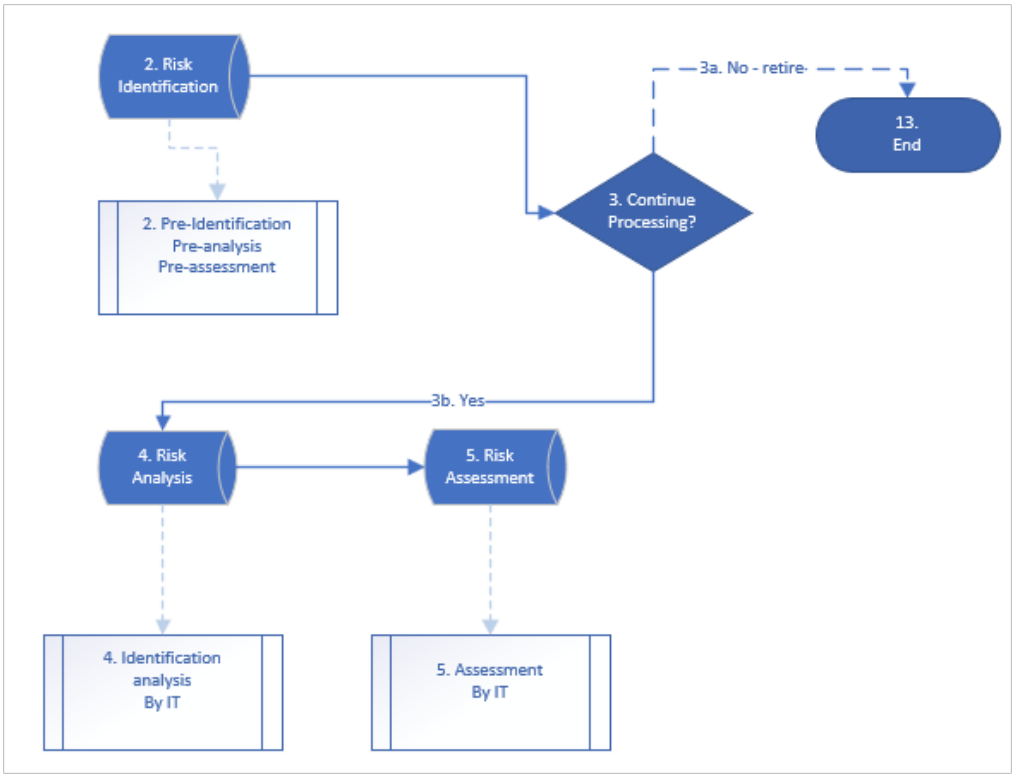


Figure 18: Research Result

Managers of the organization must assess their tolerance for risk and provide guidelines for the IT department's Risk Management accordingly. While higher risk may initially entail lower costs, the organization faces increased costs in the event of setbacks, depending on the level of risk or risks that materialize.

6.2 Identifying Assets

First and foremost, the organization must identify its assets to effectively prioritize Risk Management, focusing primarily on critical assets. Standardizing workstations can help mitigate their associated risks. In the target organization, computers do not have administrative rights to workstations, which is already an effective control measure to prevent malware spread. Microsoft E5 Security has been implemented for workstations, along with Defender for Cloud for servers. This enables monitoring of various risk levels through Microsoft's portal, thereby enhancing risk visibility.

The risk is exacerbated by the absence of a one-workstation policy. Without this policy, workstations remain inactive, leading to missed operating system and third-party application updates, such as browsers or PDF programs. Additionally, maintaining extra workstations results in increased costs.

Outdated practices persist, such as keeping End-Of-Life (EOL) servers online as a precaution, despite the adoption of modern practices. Unidentified online assets pose a threat, necessitating their identification, along with segregating other assets into more isolated networks to restrict access only to necessary services. Fortunately, there is a plan in place to address these issues.

Each unit within the organization should be capable of identifying its own assets, whether they are servers, network devices, or files on disk shares. Neglecting to acknowledge or identify the existence of a device hampers the organization's ability to prepare for and mitigate risks effectively.

6.3 Problems With the Level of Maturity

While the organization's maturity level may not currently support the full implementation of the Risk Management model, steps can be taken to gradually introduce it. Initiatives such as Risk workshops and training sessions can be conducted to increase awareness and understanding of Risk Management practices. Reminders should be provided to emphasize the importance of conducting Risk Analysis and Assessment whenever changes are proposed or assets are added to the network.

The development of Cybersecurity maturity and processes should be approached systematically, with a focus on raising employee awareness of the significance of Risk Management and Cybersecurity. It is essential to provide clear justifications for these initiatives to garner support from stakeholders. By demonstrating the tangible benefits of Risk Management in understandable terms, organizations can encourage greater participation and adoption of these practices, ultimately enhancing overall maturity in Cybersecurity and data protection.

Managers in an organization who lack the experience or inclination to address risks inadvertently create challenges for the organization. Without their support, Risk Management activities may not receive the necessary attention and commitment. Risk management typically occurs annually through workshops at the top levels of the organization. However, this information is not currently outlined in organizational policies and has not been widely adopted across the organization.

The next step should involve the development of an organization-wide Risk Management policy that mandates the implementation of a Risk Management Model throughout the organization. Additionally, several other policies may be missing or outdated and should be reviewed and updated accordingly. Regular annual reviews should be conducted to ensure that all policies remain current and reflective of Senior Management's decisions. It is also important to assess

the need for new policies regularly, as changing times and practices may necessitate updates to existing policies or the creation of new ones.

6.4 New Security Roles

The organization is in need of a Risk Management Board (RMB), which can be established as a virtual team. This virtual team may be led by either a Chief Information Security Officer (CISO) or a dedicated Risk Manager, depending on the organization's size and requirements. In larger organizations, both roles may be necessary. Currently, the RMB consists of a management team lacking expertise or experience in Risk Management. Therefore, it is essential to hire a qualified Risk Manager, who could potentially also serve as the CISO, a position currently vacant within the organization. Alternatively, the organization may opt to hire or contract both a CISO and a Risk Manager.

In addition to establishing a Risk Management Board, the organization already has a data protection virtual team in place. Therefore, it would be prudent to establish a Cybersecurity focused virtual team alongside it. Consideration could also be given to setting up an Advisory team within the organization to provide expert support to various functions and Senior Management. However, it is important to recognize that these initiatives may lead to increased costs, as the teams would require qualified specialists to effectively fulfill their roles.

6.5 Overwhelming Risk Management

Risk Management can be daunting, particularly when dealing with a large number of assets. To simplify the process, focus on managing only those assets that fall within the responsibility of each department and are critical to the organization's infrastructure. Avoid attempting to control risks that are not directly owned by a specific department.

The system owner plays a crucial role in this process and is responsible for addressing risks within their area of oversight. It's important to recognize that

system owners may require support from the IT department when managing IT-related risks. This collaborative approach ensures that risks are effectively identified, assessed, and mitigated across the organization.

6.6 Other Things to Research

Areas for further study related to Risk Management include change management, which can contribute to reducing risks within an organization's network. Additionally, the utilization of risk information in decision-making processes for service development should be explored. It's important to recognize that risk is not always negative; there are instances where it can be beneficial. When risks are managed, analyzed, assessed, or identified, new opportunities or insights may emerge that can aid in organizational development.

These positive risks, often referred to as opportunities, should also be considered within organization-level Risk Management practices. It's valuable to explore how these positive risks can be leveraged. One approach is to assess the level of risk-taking tolerance on a case-by-case basis. The organization's general Risk Management policy should provide guidance on how to navigate these situations at a broader level.

Life cycle management has begun with leasing acquisitions, allowing for the replacement of network equipment, servers, workstations, phones, and other hardware at the end of the leasing period. This approach helps minimize the risks associated with aging hardware. Further development of life cycle management practices and their implementation within the organization should be explored for future enhancement.

Artificial Intelligence (AI) should be investigated for its potential to identify and analyze risks. It would be particularly beneficial if AI could automatically retire risks with a medium or lower risk score, thereby reducing the workload on small IT departments. Additionally, the broader utilization of AI should be considered, as it has the potential to bring cost savings and impact job roles.

The implementation of a Disaster Recovery Plan (DRP) should be prioritized to provide operational guidance on restoring critical services quickly in the event of a serious failure. It's important to note that Disaster Recovery (DR) efforts alone are insufficient; they must be integrated into the organization's Business Continuity (BC) framework.

6.7 Organizational Culture

In the organization's culture, remnants of outdated practices are still prevalent, where individuals may avoid certain tasks because they are perceived as unpleasant or undesirable. Some system owners may only hold nominal roles and fail to fulfil their responsibilities adequately, often relying on the IT department or others to handle tasks on their behalf. Many roles and responsibilities within the organization need to be redefined and enforced to ensure proper execution.

Overall, the cybersecurity culture within the organization is lacking, highlighting the need for comprehensive training and potentially outsourcing certain functions. Specific actions regarding outsourcing are not determined at this stage.

Numerous teams within the organization exhibit deficiencies in documentation, processes, and collaboration. Collaboration between teams is particularly challenging due to existing silos, which hinder transparent communication and cooperation. Organizational policies should promote openness in operational practices and allow for customization to accommodate different activities. A one-size-fits-all approach is ineffective and should be replaced with flexible policies that can be tailored to specific team needs.

References

Example (Vancouver = numbering system):

1 https://medium.com/@Aircon/intro-to-defensive-security-tryhackme-cb9a580bbbf8. 2022

2 https://www.ibm.com/topics/offensive-security

3 https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

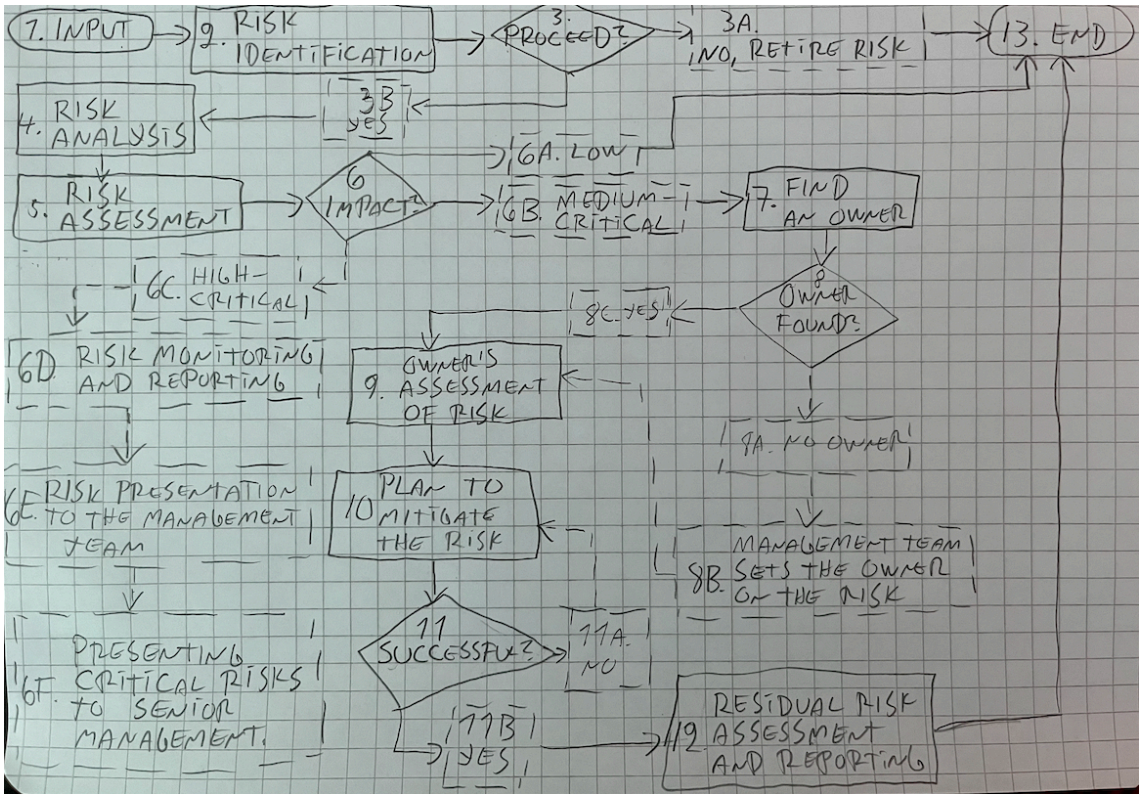
4 https://www.maltego.com/blog/understanding-the-different-types-of-intelligence-collection-disciplines

5 VAHTI Risk Management Guideline. <http://urn.fi/URN:ISBN:978-952-251-862-0>. Accessed 29 Feb 2024.

6 Harris S., Maymi F., Cissp all-in-one Exam Guide, 8th Edition. McGrew-Hill Education. 2019.

7 Miller L., Gregory P., CISSP for Dummies 5th Edition. A Wiley Brand. 2016.

Appendix 1: Initial Carbon Draft of a process



Appendix 2: Initial Risk Management Process Walk through

1. Input (Everything needs to be documented)

   This is Risk which going to cost a lot of money if it is triggered as an incident, published web service.
2. Risk Identification

   Here Risk needs to be Identified as well as Possible such as Internal and external point of views.
3. Proceed?
   a. If there would be no Risk Identified at this time or does not apply to your own organization Risk can be Retired.
   b. Risk does apply to your own organization and worth to be analyzed.
4. Risk Analysis

   There should be Risk Management team for analysis. This will be quite subjective part where everybody has chance to say an opinion how this affects to an organization.

   Excel sheet or Risk Management system can be used.
5. Risk Assessment

   Risk Assessment (Likelihood x Severity)

   Likelihood is set to 4 and severity is set to 5 so score is 20 and it is high Risk and might be critical as well depending of a point of view.
6. Impact
   a. Low: Retire and End (13)
   b. Medium – Critical.

      Only medium or medium-high; goto step (7)

      From High to Critical, Run (6c) and Go to step (7)

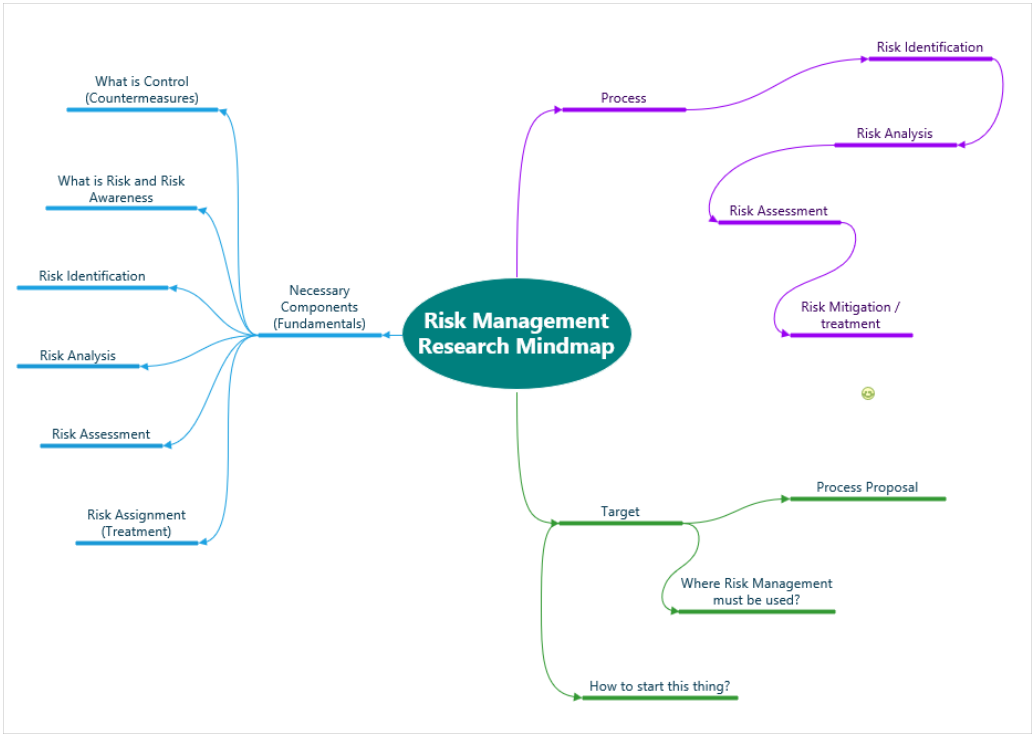
      From 6c to 6f are handled by Risk Management Board (RMB) and board will inform all parties how this is proceeding.
   c. High to critical needs to be reported to Responsible person of Risk Management, should be Risk Management board.

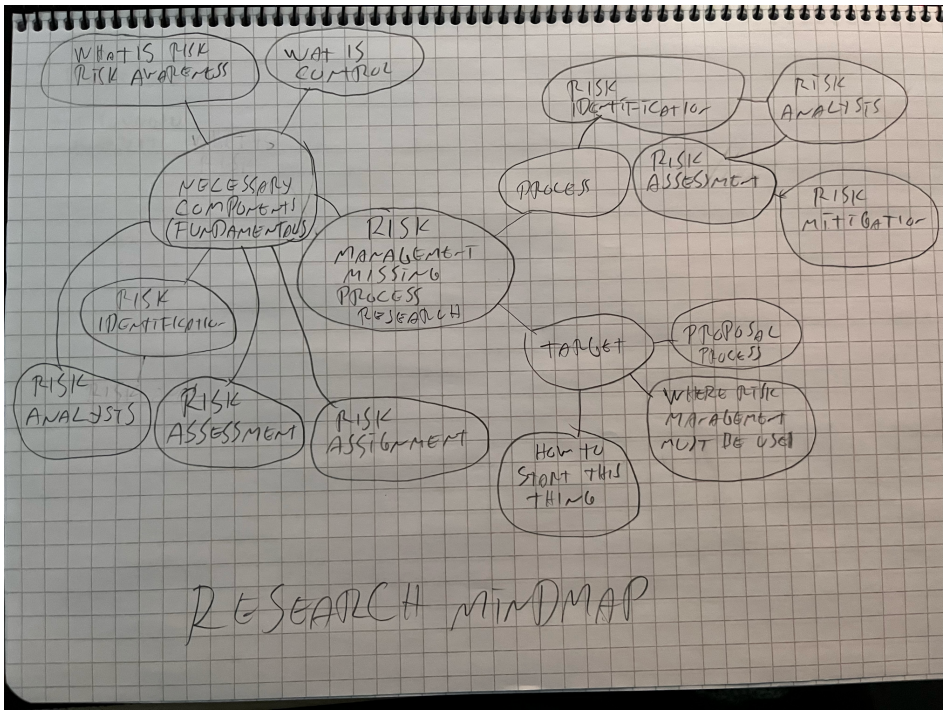
d. RMB will monitor and report risk(s) after these Risk are re-evaluated by RMB members and need to figure out if some budget is needed to fix it.
e. Risk(s) reported to the Management team and informed how this is going to be fixed (note: use specialist if necessary) and all possible costs. And what this can cost if not fixed.
f. If this is Critical Risk and can impact widely to whole organization and incapacitating big parts of organization or hits to reputation or similar. Then this risk(s) must report to the Senior Management.

7. Find an Owner
   Owner is needed who can make calls what to with the system.
   Owner most likely needs help from IT-team when managing risks.
   Incident Response Manager (IRM) makes decisions as well if necessary.
   Major Incident Manager (MIM) calls shots immediately without an owner.
8. Owner found?
   a. No owner set, go to (8b)
   b. Management team finds owner for the system.
   c. Yes, owner found go (9)
9. Owner's Assessment of Risk with specialist(s)
   Specialist from IT- department and from Vendor.
10. Plan to and how to mitigate (reduce) Risk.
    Risk mitigation, Risk Assignment, Risk Avoidance, Risk Acceptance
11. Was it successful?
    This means did team made valid action and Risk is mitigated.
    Software updated, configuration changes, removing unnecessary parts of software etc.
    a. No, failed. Find other specialist if current team cannot Find solution.
    b. Yes, mitigation was successful (document the solution) go to (12)
12. Residual Risk Assessment and Reporting. Go to (13)
13. This is end.
    Risk is mitigated set it to Monitor state.

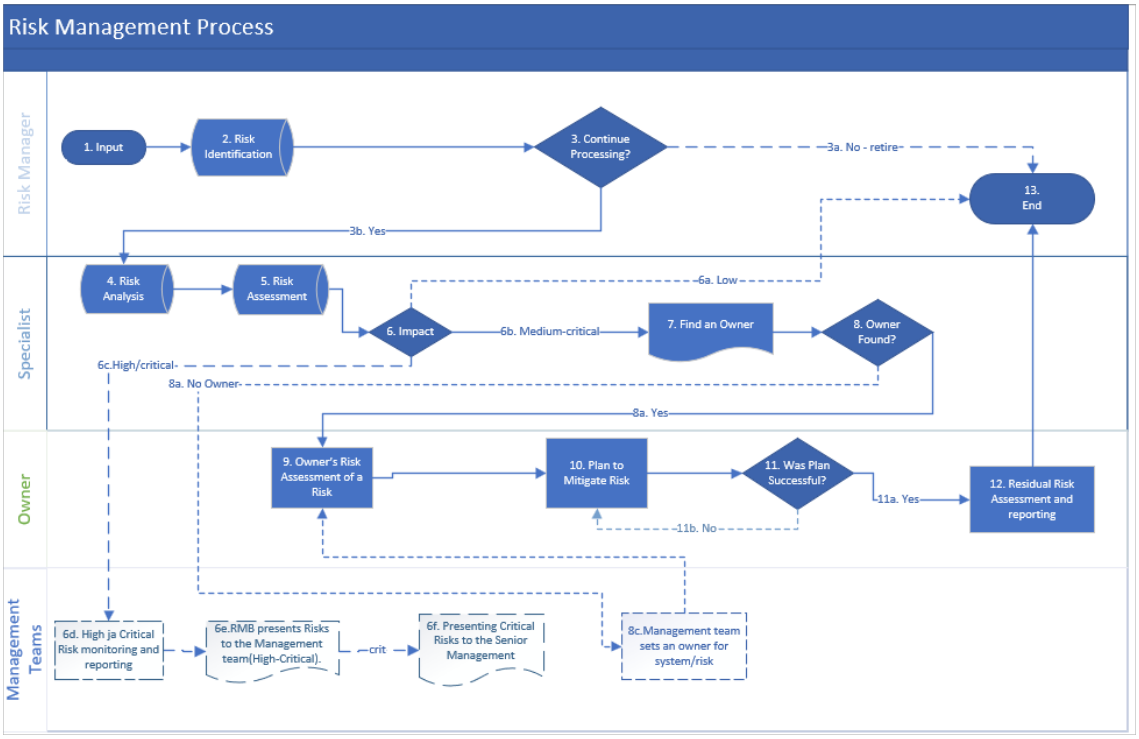
No actual Risk, set it to Retire State

Appendix 3: Mindmaps





Appendix 4: Swimlane Risk Management Process



Appendix 5: Risk Management Process Walk through (Tables)

Risk Identification

Table 1: Risk Input

Action	Information	Case Path
(1) Input	This input can be any employee by name or anonymous channel or workshop.	

Table 2: Risk Identification

Action	Information	Case Path
(2) Risk Identification	Their Risk needs to be Identified as well as Possible by Risk Manager.	

Table 3: Decision 1: Proceed?

Action	Information	Case Path
(3a) Proceed (no) (13) END	if there would be no Risk Identified at this time or does not apply to an organization Risk can be Retired. This would go to (13) END. Must be documented as well.	
(3b) Proceed (yes)	Risk does apply to an organization and worth to be analysed.	

Risk Analysis

Table 4: Risk Analysis

Action	Information	Case Path
(4) Risk Analysis	Members try to come up with possible negative and positive perspectives on risk	

Table 5: Risk Analysis Breakdown

Analysis	**Control needed**	**Control**

Risk Assessment

Table 6: Risk Assessment

Action	**Information**	**Case path**
(5) Risk Assessment	Risk Assessment (Likelihood x Severty) Likelihood is set to 4 and severity is set to 5 so score is 20 and it is high Risk and might be critical as well depending on a point of view.	

Table 7: Decision 2, Risk Impact

Action	**Information**	**Case Path**
(6a) Low Risk impact	Retire and End (13)	
(6b) Medium – Critical risk impact	medium or medium-high; goto step (7) High-Critical steps (6c) and (7)	
(6c) High-Critical impact	High to critical needs to be reported to Responsible person of Risk Management, should be Risk Management board (6d)	
(6d) RMB monitors risk and report risk	RMB will monitor and report risk(s) after these Risk are re-evaluated by RMB members and need to figure out if some budget is needed to fix it. (6e)	
(6e) High-critical impact	Risk(s) reported to the Management team and informed how this is going to be fixed (note: use specialist if necessary) and all possible costs. And	

	what this can cost if not fixed. If critical or decided (6f)	
(6f) Critical Risk impact	If this is Critical Risk and can impact widely to whole organization and incapacitating big parts of organization or hits to reputation or similar. Then this risk(s) has to report to the Senior Management.	

Table 8: Find an Owner

Action	**Information**	**Case Path**
(7) Find an Owner	Owner is really needed who can make calls what to do with the system. Owner most likely needs help from IT-team when managing these risks. Incident Response Manager (IRM) can make decisions as well if necessary. Major Incident Manager (MIM) calls shots immediately without consulting an owner.	

Table 9: owner found?

Action	**Information**	**Case Path**
(8a) No	No owner set, go to (8b)	
(8b) Management team set an owner	Management team finds owner for the system	
(8c) yes	owner found go (9)	

Table 10: Owner´s assessment of risk

Action	**Information**	**Case path**
(9) Owner's Assessment of Risk	Owner should use specialist from vendor and from IT-department	

Risk Mitigation

Table 11: Plan to Mitigate the Risk

Action	Information	Case Path
(10) Plan to mitigate (reduce) Risk	Plan to and how to mitigate (reduce) Risk. Risk mitigation, Risk Assigment, Risk Avoidance, Risk Acceptance	

Table 12: Mitigation plan Successful?

Action	Information	Case Path
(11a) No	Team did not build valid Mitigation plan. Find other specialist if current team cannot Find solution.	
(11b) yes	mitigation actions were successful go to (12)	

Table 13: Residual Risk

Action	Information	Case Path
(12) Residual Risk Assessment	There is always residual risk which needs to be assessed and reported. After implementing new controls or alter current controls assessment needs to be redone.	

Table 14: End of Process

Action	Information	Case Path
(13) End		
(3a)	No Actual Risk. Retire and report.	
(6a)	Low Risk. Monitor or retire based on policy.	