UPPSALA
UNIVERSITET

UPTEC STS 19017
Examensarbete 30 hp
Juni 2019

# The MaRiQ model: A quantitative approach to risk management in cybersecurity

Elin Carlsson
Moa Mattsson

UPPSALA
UNIVERSITET

**Teknisk- naturvetenskaplig fakultet**
**UTH-enheten**

Besöksadress:
Ångströmlaboratoriet
Lägerhyddsvägen 1
Hus 4, Plan 0

Postadress:
Box 536
751 21 Uppsala

Telefon:
018 – 471 30 03

Telefax:
018 – 471 30 00

Hemsida:
http://www.teknat.uu.se/student

# Abstract

## The MaRiQ Model: A quantitative approach to risk management in cybersecurity

*Elin Carlsson & Moa Mattsson*

In recent years, cyber attacks and data fraud have become major issues to companies, businesses and nation states alike. The need for more accurate and reliable risk management models is therefore substantial.

Today, cybersecurity risk management is often carried out on a qualitative basis, where risks are evaluated to a predefined set of categories such as low, medium or high. This thesis aims to challenge that practice, by presenting a model that quantitatively assesses risks - therefore named MaRiQ (Manage Risks Quantitatively).

MaRiQ was developed based on collected requirements and contemporary literature on quantitative risk management. The model consists of a clearly defined flowchart and a supporting tool created in Excel. To generate scientifically validated results, MaRiQ makes use of a number of statistical techniques and mathematical functions, such as Monte Carlo simulations and probability distributions.

To evaluate whether our developed model really was an improvement compared to current qualitative processes, we conducted a workshop at the end of the project. The organization that tested MaRiQ experienced the model to be useful and that it fulfilled most of their needs.

Our results indicate that risk management within cybersecurity can and should be performed using more quantitative approaches than what is praxis today. Even though there are several potential developments to be made, MaRiQ demonstrates the possible advantages of transitioning from qualitative to quantitative risk management processes.

Handledare: Emelie Eriksson Thörnell & Martin Bergling
Ämnesgranskare: Björn Victor
Examinator: Elísabet Andrésdóttir
ISSN: 1650-8319, UPTEC STS 19017
Tryckt av: Uppsala

# Sammanfattning

Cyberattacker och databedrägerier har under det senaste decenniet blivit allt vanligare företeelser. I takt med att samhällen digitaliseras och fler företag, organisationer och privatpersoner drar fördelar av att vara uppkopplade mot olika nätverk ökar riskerna för att data hamnar i orätta händer och att informationsteknologiska system inskränks av obehöriga.

Vissa menar att lösningen på dessa problem är att införa mer innovativa och tekniska åtgärder så som nätverksövervakning och konfigureringspolicies. Denna rapport tar en annan approach till problemet. Precis som ett växande antal forskare och sakkunniga menar vi att det behövs någonting mer än teknik för att trygga våra IT-system. Detta ”något” är mer vetenskapliga och tillförlitliga riskhanteringsmodeller.

Idag utvärderas risker inom cybersäkerhet ofta kvalitativt, där riskerna subjektivt bedöms mot ett antal förbestämda kategorier så som *låg*, *medium* och *hög*. Trots att metoden är vanligt förekommande medför den flera allvarliga problem. Hur vet vi exempelvis vilken risk som ska prioriteras om två är kategoriserade som höga? Och vem avgör vad den objektiva skillnaden mellan en låg- och mediumklassad risk är?

Syftet med denna studie är att bemöta problemen med den kvalitativa riskbedömningen genom att ta fram en ny, *kvantitativ* riskhanteringsmodell. Projektet utfördes i samarbete med cybersäkerhetsföretaget Nixu och modellen som tagits fram är anpassad till deras verksamhet och kunder. Modellen är kvantitativ på så sätt att den grundar sig i intervallskattningar kring riskernas procentuella sannolikhet att inträffa och monetära konsekvenser. Genom att utnyttja statistiska tekniker och matematiska funktioner, så som Monte Carlo-simuleringar och sannolikhetsfördelningar, genererar modellen resultat som är mer vetenskapligt grundade än de kvalitativa riskbedömningarna. Den utvecklade modellen har namngivits MaRiQ eftersom dess syfte är att hantera risker kvantitativt, på engelska: *Manage Risks Quantitatively*.

MaRiQ består av ett tydligt definierat processflöde och ett digitalt verktyg, utvecklat i Excel, som stöttar användarna i riskhanteringsprocessen. För att undersöka hur väl processflödet och verktyget fungerar genomfördes en workshop med en av Nixus kunder i projektets slutskede. Utfallet av workshopen var att kunden upplevde att modellen var både genomförbar och användbar och att de resultat som genererades ansågs mer trovärdiga än de kvalitativa riskbedömningarna.

Slutsatsen av studien är att det både är möjligt och lämpligt att bedriva riskhantering inom cybersäkerhet på mer kvantitativa grunder än vad som är praxis idag. Trots att MaRiQ har en stor utvecklingspotential, påvisar modellen redan i detta skede att det finns flera fördelar att vinna på en transition från kvantiativ till kvalitativ riskhantering. Vi hoppas därför att vår modell kan tjäna som en inspiration för framtida kvantiativa riskhanteringsmodeller.

# Acknowledgements

Through the writing of this thesis, we have received a great deal of support and assistance. First, we would like to express our deepest gratitude to our supervisors at Nixu: Emelie Eriksson Thörnell and Martin Bergling. Your continuous support and passionate participation have carried us further than we thought possible. Together with additional staff at Nixu, you have provided relevant insights and unceasing encouragement and your professional guidance has been of great value to us.

We would also like to thank Björn Victor, our academic supervisor at Uppsala University. Björn steered us in the right direction when the road ahead seemed hazy and helped us forward the project by answering questions about our research and writing.

A special thanks also goes out to all individuals who have participated in interviews, surveys and workshops to further our work. Without your input, the development and validation of the MaRiQ model would not have been possible.

Finally, we would also like to acknowledge family and friends who have been of great support in deliberating over our problems and findings. Thank you for your wise counsel, for your patience and sympathetic ears.

To all of you, our most sincere thank you.

Elin Carlsson & Moa Mattsson
Uppsala, Sweden
June, 2019

# Table of Contents

# 1. Introduction

On the 18th of February 2019, the web-magazine Computer Sweden published a worrisome article. According to the reportage, 2.7 million recorded phone calls to the Swedish telephone-based healthcare provider 1177 Vårdguiden were publicly stored on unprotected web servers, available to download for any interested party (Dobos, 2019). As the story unfolded, it stood clear that the subcontractors of 1177 had their servers placed abroad and that the most likely explanation for the incident was that someone had accidentally put a network-cable into the hard drive where patient data was stored (Dagens Nyheter, 2019). Even though no evidence has yet been found indicating that data was stolen, the 1177-incident clearly points to the risks associated with digital information storage and gives us a glimpse of what kind of data hackers could gain access to in the future (Ny Teknik, 2019).

The incident at 1177 is only one of several examples of IT-breaches and ruptures that have occurred during the recent decade. According to The Global Risk Report, published by The World Economic Forum in 2018, attacks against businesses have almost doubled in the last five years and events that used to be considered extraordinary are now becoming commonplace. According to the same report, cyber attacks and data fraud or theft are ranked as number three and four respectively on the top 5-list of current global risks in terms of likelihood (following extreme weather events and natural disasters) (World Economic Forum, 2018).

So, is this the end of the line? Have cybercriminals gained control of the digital arena and all we can do is close our eyes and hope for the best? Of course not. Several studies point to the fact that most cyber incidents and data breaches can actually be avoided, having the right protection and understanding of the situation (Zetter, 2009; Online Trust Alliance, 2018). Many argue that the best way to enforce countermeasures is to introduce better and more innovative technology, such as proper configuration policies and network monitoring (Zetter, 2009; Hubbard and Seiersen, 2016, p.3). The argument posed in this thesis follows a different approach. Just as an emerging number of cybersecurity professionals, we believe that there is something more than technology needed when aiming to effectively battle cybersecurity threats. That “something” is more accurate and predictive risk management models.

As of today, risk management has become an integrated part of many organizations’ daily practices to mitigate cyber threats. How the risk management process is carried out differs from organization to organization, but the one commonality is the objective to prioritize risks in order to decide on how to allocate limited resources. To prioritize, the vast majority of organizations resort to some sort of scoring system, where each risk is evaluated to a predefined set of categories. A standard approach is to rate risks in terms of *likelihood* and *impact*, often on a scale varying from low to high and plot each risk in a matrix having likelihood and impact on the axes. The basic idea is that risks having higher scores are more critical to handle and that they should, therefore, be prioritized (Andersson *et al.*, 2011; Hubbard and Seiersen, 2016).

Even though this qualitative approach to risk management has been endorsed and promoted by numerous major organizations, such as the International Organization for Standardization (ISO) and the Open Web Application Security Project (OWASP), it poses several issues that need to be addressed. This paper will describe these problems and how we have approached the issue of qualitative risk management by developing our own *quantitative* model, suitable for use at the cybersecurity consultant firm Nixu.

The resulting risk management model was named MaRiQ since its purpose is to Manage Risks Quantitatively. MaRiQ consists of a process flowchart and a supporting software tool, that helps the user perform the needed computations. The model is based on already existing risk management frameworks and on material collected during interviews with cybersecurity professionals, concerning their perceptions of successful risk management models. In this paper, we will describe MaRiQ and its supporting tool, along with the theoretical basis upon which it has been built. We will also outline how we tested our model in a real-life scenario with one of Nixu's customers.

The results of our work indicate that risk management within cybersecurity can and should be performed using more quantitative approaches than what is common practice today. Our developed model was welcomed by the organization who tested it as they expressed that MaRiQ was useful and viable and provided more informative results than qualitative counterparts. As will be described in the final section of this paper there are several ways in which our developed model can be improved. However, as our results show, these potential developments are also dependent on the cybersecurity community reaching a more mature level of understanding for risk management. Based on the results achieved from this study, our firm belief is that incidents like the one at 1177 can be avoided, having a better understanding of risk management and more accurate methods for evaluating potential risks.

## 1.1 Purpose and limitations

The purpose of this project is to create a quantitative risk management model. The model is to be used by consultants working at the cybersecurity services company Nixu, when conducting risk management workshops and assessments in collaboration with customers. Hence, the target group of the model is Nixu's customers, ranging from a variety of areas such as banking- and forestry industry to public sector actors. The model will serve as an operational cybersecurity risk management instrument that can be broadly applied, irrespective of the type of organization at stake.

To ensure that we fulfil the ambitions of this thesis, the above-stated purpose has been reformulated into three explicit research objectives of this study:

- To survey available risk management models used within the cybersecurity community,

- To develop a quantitative risk management model, attuned for Nixu and its customers, and

- To produce a software tool that supports the model.

The thesis is limited in the sense that it will only consider *cybersecurity* risk management. This means that we will not attempt to draw any broader conclusions regarding risk management in general. Neither will information regarding risk management be collected from other research fields, even though there are numerous candidates available such as finance or insurance business.

## 1.2 Disposition

The thesis consists of four major parts. In the first part, we will introduce the reader to the field of cybersecurity risk management by providing a background to the topic of quantitative risk management as well as presenting previous work relating to ours. The second part concerns formalities of the thesis, meaning that we will present the methodological foundations upon which we have chosen to build our model as well as the statistical framework within which it is created. The third part of the thesis outlines what would usually be referred to as *results.* Here we will present collected model requirements, the compiled theoretical model framework and lastly the constructed model itself. In the last part of the thesis, we will reflect upon our work and present ideas for how the model can be improved in the future.

In summary, the disposition of the thesis can be described as follows:

- **Part I:** Introduction to the field of quantitative risk management, sections:
    - *2 Background* and
    - *3 Related work*
- **Part II:** Formalities of the thesis, sections:
    - *4 Methodology* and
    - *5 Statistical aspects of risk management modelling*
- **Part III:** Results, sections:
    - *6 Model requirements*
    - *7 Core activities* and
    - *8 The MaRiQ Model*
- **Part IV:** A look in the rear-view mirror, sections
    - *9 Discussion* and
    - *10 Conclusion*

## 1.3 Collaborating partner: Nixu Cybersecurity

This thesis has been written in collaboration with the consultant firm Nixu Cybersecurity. Nixu is a cybersecurity services company whose stated mission is to "[…] keep the digital society running" (Nixu Cybersecurity, 2019). The company was founded in Finland in 1988 and has since expanded its businesses to Sweden and the Benelux Union (Nixu Cybersecurity, 2019). Cybersecurity risk management is a central area of interest at Nixu and the company has experienced a great need among its customers for more efficient and accurate risk management models, where quantitative measurements are part of the assessment.

Nixu is a suitable partner for a thesis of this kind since the company has previous experience of working with risk management within the cybersecurity community, as well as knowledgeable employees with the right set of skills for supporting a master thesis of this type. Nixu's primary role in this project has been to provide information about current risk management practices within the area as well as supporting and revising the work with this thesis.

# 2. Background

The idea to quantify and control cybersecurity risks has been around since the early 1960s. What started as an initiative from the U.S Department of Defence to assure the security of military computer systems, soon spread to civilian governments and corporations around the world (Slayton, 2015). Today, risk management is viewed as an essential element of good governance and an integral part of management practices to achieve adequate computer security at the lowest possible cost (European Union Agency for Network and Information Security [ENISA], 2019). This section will cover the contemporary debate of whether risk management should and could be based on quantitative values, but before getting into the details, let us start with the basics by answering the question: what is risk management?

## 2.1 What is cybersecurity risk management?

In order to understand the process and implications of risk management, we need to begin with a short discussion on the term *risk.* There are numerous descriptions of risk available in the literature and every author seems to add his or her own flavour to the definition (Freund and Jones, 2014, p.3). The general phrasing often ends up somewhat similar to the definition given by Douglas Hubbard, author of the pioneering book *How to measure anything: Finding the Value of Intangibles in Business*, of risk as:

> *A state of uncertainty where some of the possibilities involve a loss, catastrophe or other undesirable outcome* (Hubbard, 2014, p.29).

This description is the general definition of risk that will be used throughout this thesis. Risk can also be defined in more measurable terms, as the combination of *the likelihood of an event occurring* and *the potential impact connected to that particular event* (Curtis and Carey, 2012). The result of this function of likelihood and impact is commonly referred to as *risk level* (ISO 27005, 2018). Quantitatively, the risk level is often expressed in terms of *expected loss (EL),* and for a risk X, it can be mathematically formulated as in Equation 1 (Wolke, 2017, p.12):

$$EL(X) = Likelihood(X) \cdot Impact(X) \qquad (1)$$

Now that we have a fundamental understanding of the term risk, we will turn to the larger discussion on risk management. Risk management is a process where activities are coordinated to "[…] direct and control an organization with regards to risk" (ISO 31000, 2018). The goal of the risk management process is to maximize the output of the organization, in terms of for example services, revenue, and products, while still minimizing the chance for unexpected outcomes (Wheeler, 2011, p.7). In order to perform risk management, a systematic approach to the process is needed which allows the analyst to understand what can happen, how likely it is, which the possible consequences are and what should be done to reduce the risk to an acceptable level. One such established systematic

approach to cybersecurity risk management is described in the International Organization for Standardization's (ISO) standard 27005:2018 *Information technology - Security techniques - Information security risk management.*

The ISO definition of cybersecurity risk management is illustrated in Figure 1 and contains eight main activities, two decision points, and several arrows, explaining the flow of information through each activity. To give the reader a basic intuition of what a cybersecurity risk management process may look like, each of the eight activities will be briefly outlined below according to the ISO 27005 standard.

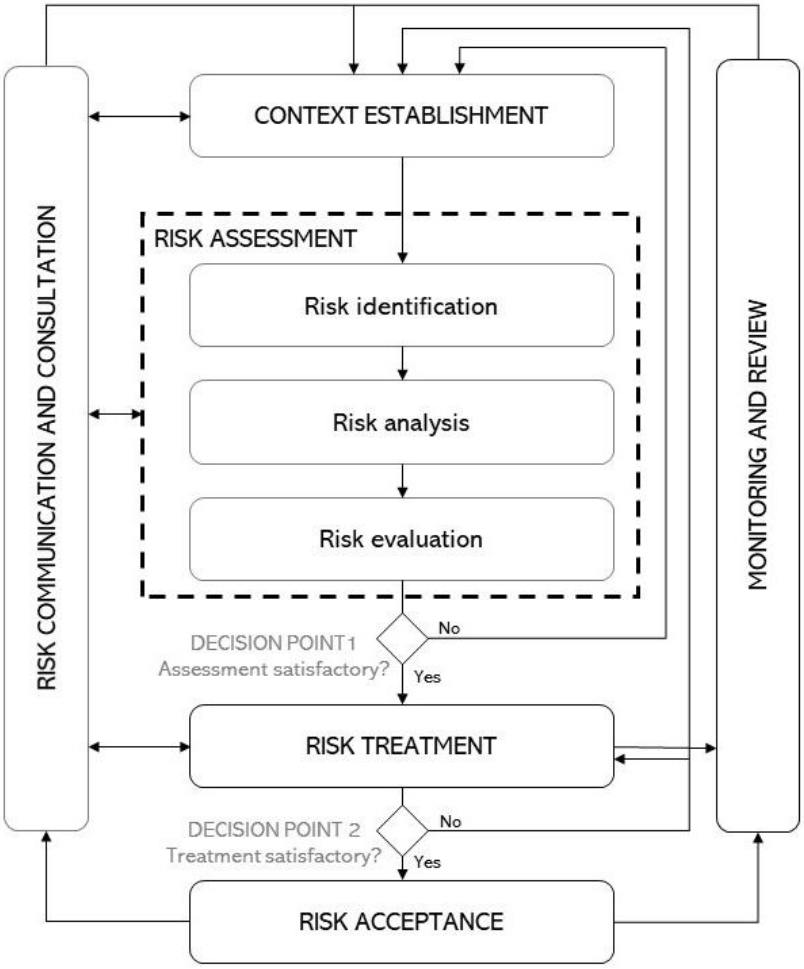



*Figure 1: Illustration of a cybersecurity risk management process (ISO/IEC, 2018, p.9).*

The first step in the cybersecurity risk management process is *context establishment*. Questions like "What system are we assessing?" and "How much risk are we willing to accept?" should be clearly answered in this first phase of the process. Having determined the context and the risk acceptance criteria, also called risk tolerance, the next step is to *assess* the risks through three sub-processes: risk identification, risk analysis, and risk evaluation.

Hence, the second phase of the risk management process is *risk identification*. This is a crucial part of the process since the risks identified here will construct the basis upon which the rest of the assessment lies. The output of the identification process should be a list of clearly defined risks with related consequence-descriptions and assets.

The third step of the process is *risk analysis.* A risk analysis can either be qualitative or quantitative (or a combination of both) and after deciding on which methodology to use, two parameters need to be assessed: the consequence of each risk and the likelihood that it will happen. The risk level must also be determined, that is to put a value on each of the assessed risks based on its consequence and likelihood, for example by calculating the expected loss.

The next step in the process is *risk evaluation.* Here, the level of risk is compared against the risk tolerance, that was established during the initial phase of the process, to see if the risk passes or not. The process also entails comparisons between different risks based on their established risk level.

Given that the results from the risk assessment are satisfactory, the next step is *risk treatment*. According to the ISO definition, there are four options available for risk treatment: risk modification (reduce the level of risk until acceptable), risk retention (accept and budget for the level of risk), risk avoidance (eliminate the activity that give rise to the particular risk) and risk sharing (share or transfer the risk to another party, for example through insurances).

Finally, the last step of the process is *risk acceptance* where the remaining risks are accepted or declined, and decisions are made regarding responsibilities for the implementation of the decided treatments.

As shown in Figure 1 there are also two continuously running processes in the cybersecurity risk management process: *risk communication and consultation* and *monitoring and review.* The purpose of these activities is to share information between different stakeholders in the process as well as to routinely identify changes in the context of the organization to maintain an overview of the complete risk picture (ISO 27005, 2018).

## 2.2 What are the challenges in cybersecurity risk management?

Despite the relatively straight forward ISO description of risk management presented in Figure 1, the process of managing risks in cybersecurity is not as simple as it might seem. There are several reasons as to why this is a difficult task for many organizations. Below, we will outline some of the challenges in contemporary cybersecurity risk management.

*i.* *Cybersecurity does not obey the physical laws of nature*
Unlike traditional forms of engineering, software engineering has no foundation in physical laws. Phenomena such as automation, scaling, and replication can occur in the world of software as in no other field. Therefore, the risk of introducing

uncertainty and other sources of failure into a cybersecurity context is greater than in other types of businesses (Haimes, 2015, p.24).

ii. *The ever-changing risk landscape*
A risk assessment can never be more than a representation of the reality you think exists today. The cybersecurity risk landscape is constantly changing and tomorrow there might be a new wave of computer hacking attacks that could completely change the way you look upon the situation. The rapidly shape-shifting risk landscape is a real challenge to cybersecurity risk management and analysts must therefore always keep an ear to the ground not to miss out on any relevant changes (Freund and Jones, 2014, p.17).

iii. *The ever-growing attack surface*
Due to the fact that more and more organizations, companies and private persons alike are finding efficiencies from being connected to different networks, the global *attack surface* for hackers and other cybercriminals have grown at a fast rate. An attack surface can be defined as the total of all exposures of an information system, which exposes value to untrusted sources (Hubbard and Seiersen, 2016, p.9). Your home, your bank account, your family and your identity nowadays all have a digital attack surface and as the surface grows, so does the need for comprehensive and evasive risk management models (Hubbard and Seiersen, 2016, p.9-11).

iv. *The difficulty in creating universal solutions*
Since there is a multitude of evolving cyber threats varying in size and complexity as well as a large variety of organizational types, it is hard, if not to say impossible, to create a universal solution to the risk management problem suitable for all types of threats and organizations (Wheeler, 2011).

v. *The complexity of risk vectors*
Cybersecurity is often viewed as primarily an IT-problem, but fact is that it is just as well a people, process and leadership problem. Calculating cyber risk is therefore relatively complex since it requires a number of vectors that range from likelihood and potential impact to human behaviour and organizational assets (Goel, Haddow and Kumar, 2018).

vi. *The redundancy of available models*
Today, hundreds of cybersecurity risk management models and academic security modelling frameworks exist (Dubois *et al.*, 2010, p.290). This redundancy of available models makes it hard for many organizations to select the most suitable approach and decide on how to proceed or start their risk management process (Dubois *et al.*, 2010; Goel, Haddow and Kumar, 2018, p.35).

vii. *The lack of standardized terminology*
Even though risk management within cybersecurity is nowadays common practice dating back more than 50 years, the field still suffers from a lack of standardized

terminology. When skimming through the existing body of knowledge regarding cybersecurity it is evident that risk experts have yet to conform on how to use fundamental terms such as *risk*, *threat*, and *vulnerability* (The Open Group, 2013b; Freund and Jones, 2014)

## 2.3 What is the problem with qualitative risk analysis?

As shown in section *2.2 What are the challenges in cybersecurity risk management?*, cybersecurity risk management is a clearly complex task. Therefore, it is perhaps not surprising that many organizations have chosen to prioritize simplicity over intricacy. In a risk management context, simplicity is often referred to as the use of a best practice approach where risks are evaluated using descriptive scales such as *low*, *medium* or *high* (Hubbard and Seiersen, 2016 p.85; Swedish Standard Institute, 2018). This type of analysis is what is called *qualitative*, and is often implemented due to the fact that it is easy to understand by all personnel and can be introduced to the organization relatively fast (Wheeler, 2011, p.39; Swedish Standard Institute, 2018). But the qualitative approach to risk management also poses several questions that need to be raised, for example: How do we assure that high risks for one analyst do not mean something different for another? Can we really be sure that it is better to mitigate one high risk instead of, for example, two medium ones? And in cases where there are several high-labelled risks, how do we know which ones to prioritize?

In order to understand what the problems with qualitative risk analyses are, we need to start from the beginning. In all forms of risk management - no matter if the process concerns cybersecurity, finance, governance or any other business - a method of measurement needs to be defined. That is, we need to state *how* we aim to evaluate the object, system or process of interest. When using a qualitative approach to risk management, the analysts usually try to estimate the likelihood and severity of an undesired event by choosing a value from a predefined set of categories. These choices are often limited to four or five categories, such as estimating likelihood as *likely, occasional, seldom* or *improbable* and impact as *negligible, minor, moderate* or *critical* (Hewitt and Pham, 2018). Using theoretically correct terms, this form of measurement is called an *ordinal* scale (Teorell and Svensson, 2007).

The ordinal scale is one of four existing measurement scales: nominal, ordinal, interval and ratio. Briefly, one can say that the difference between these four scales is that nominal scales cannot demonstrate ranking among the variables (e.g.: professions, sex or colours), whereas ordinal scales do provide a ranking, but cannot tell the difference between two points on the scale. For example, we know that *critical* is a higher form of impact than *moderate*, but we cannot say for certain how much of a change going from moderate to critical actually implies (The Open Group, 2009). Interval scales express the distance between two points on the scale but have no zero-point which makes it impossible to talk about relative differences such as twice as much or half of (e.g.: dates and temperatures in Celsius). The ratio scale, on the other hand, has an absolute zero-point which enables comparisons between different variables

and thereby all forms of mathematical expressions (e.g.: height and time) (Teorell and Svensson, 2007).

What then, does the ordinal scale imply for qualitative risk management? Let us show you with an example, based on the recommendations provided by Andersson et al. (2011) at the Swedish Civil Contingency Agency (MSB), of how a qualitative assessment should be carried out. Before getting into the details, we should mention that the result of the analysis in the example is presented in a *risk matrix* (also known as a heatmap or risk map), which is the standard way of visualizing the results from a qualitative risk assessment. In a risk matrix, risks are categorized according to their impact and likelihood and often marked in colours, such as red, yellow and green, to demonstrate their severity (Andersson *et al.*, 2011).

**EXAMPLE 1**

Let us say that you are a leading risk analyst at a company aiming to prioritize risks using a qualitative risk management approach. A working group has been established for the assessment and after thorough discussions, the definitions of the categorized impact and likelihood, found in Figure 2, are recognized.

| | | | Impact (SEK) | | | | |
|---|---|---|---|---|---|---|---|
| | | | Negligible | Minor | Moderate | Critical | Catastrophic |
| | | | ≤100 000 | >100 000 to 1 million | >1 million to 10 million | >10 million to 100 million | >100 million |
| Likelihood | Frequent | >99% | Medium | Medium | High | High | High |
| | Likely | >50%-99% | Medium | Medium | Medium | High | High |
| | Occasional | >25%-50% | Low | Medium | Medium | Medium | High |
| | Seldom | >1%-25% | Low | Low | Medium | Medium | Medium |
| | Improbable | ≤1% | Low | Low | Low | Medium | Medium |

*Figure 2. Example of risk matrix with high, medium and low risks (based on Andersson et al., 2011, p.15, and Hubbard and Seiersen, 2016, p.90).*

The working group has identified two risks, risk A and B, and as the leader of the assessment, you help the group position these two risks in the risk matrix. After long discussions, the group concludes that risk A is most likely to have a *critical* impact and an *occasional* likelihood. It is also estimated that risk B has an equal impact as risk A but a higher likelihood, and the group, therefore, decides to position risk B as *critical* and *likely*. Hence, based on this qualitative assessment, the risk level of risk A is medium (yellow) and for risk B it is high (red). You conclude the risk management process by identifying suitable treatments for the risks and by providing a summary of your findings to management. Your

suggestion is that risk B should be prioritized since it has a risk level that is labelled high/red, whereas risk A is only rated as a medium/yellow risk.

---

As shown in Example 1, the qualitative analysis provides results that are fairly easy to overview, comprehend and draw conclusions from. But one should be careful before saluting the simplicity of the qualitative method. It also brings several issues that need to be addressed, perhaps the most prominent one being the fact that ordinal scales come with severe mathematical limitations (Cox, 2008).

Let us say that the true values behind risk A and B in Example 1 are the following:

*Risk A:* Likelihood is 50 % and impact is 90 million SEK
*Risk B:* Likelihood is 60 % and impact is 20 million SEK

Provided these values for impact and likelihood, risk A and B would still be plotted in the same cells in the risk matrix as they were in Example 1 (that is, risk B would be considered a high/red risk whereas risk A would be considered a medium/yellow one). However, when using Equation 1 for calculating the quantitative risk level for each risk, one can see that the expected loss for risk A is $(0.5 \cdot 90 =)$ 45 million SEK, whereas the expected loss of risk B is $(0.6 \cdot 20 =)$ 12 million SEK. According to the quantitative analysis, it is therefore much more reasonable to prioritize risk A over B, which is the opposite of the result from the qualitative analysis (Hubbard and Seiersen, 2016, p.90). These calculations clearly point to the mathematical limitations of ordinal scales: it simply does not make sense to multiply occasional by moderate and expect to get a mathematically consistent answer. The results will not be reliable since qualitative scales are by definition constructed around discrete, descriptive values, subjectively defined by the working group (Hubbard and Seiersen, 2016, p.92). Tony Cox, PhD in risk analysis at MIT, goes as far as stating that these mathematical limitations make the risk matrix “worse than useless” (Cox, 2008, p.500).

Another deficiency of qualitative models, relating to the previously mentioned, is that which Cox calls *range compression*. Range compression refers to the fact that the risk matrix not only plots risks that are in opposite order by quantitative expected loss but also lumps together risks that are very dissimilar. Let us say for example that we have a risk C with likelihood 2 % and impact 10 million SEK which gives an expected loss of $(0.02 \cdot 10 =)$ 200 000 SEK, and a risk D with likelihood 20 % and impact 100 million SEK, providing an expected loss of $(0.2 \cdot 100 =)$ 20 million SEK. Based on this analysis, risk D would have 100 times the risk level as C. Yet, if using the matrix given in Example 1, risks C and D would actually be plotted in the same cell (Cox, 2008, p.506).

These mathematical inconsistencies are not the only thing that should make us sceptic towards using qualitative measurements in risk management. Several authors have pointed to the fact that ordinal scales also bring communicative problems. The psychologist David Budescu is one of them, and in a report produced for the Intergovernmental Panel on Climate

Change (IPCC), he and his colleagues investigate issues relating to how we use words to describe likelihood. The researchers set up an experiment consisting of 223 volunteers, where each of them was asked to provide their best estimate of the probabilities hiding behind the terms *very likely*, *likely*, *unlikely* and *very unlikely*. Their findings were quite remarkable, stating that very likely could mean anything from 43% to 99% probability depending on who you asked, whereas unlikely meant 8 % probability to some people and as high as 66 % to others (Budescu, Broomell and Por, 2009). Budescu summarises the implications of this varying understanding of ordinal categories in the expression *illusion of communication*. By this, he means that qualitative risk management models often create a feeling among people that they are communicating risks when, in reality, they are not in an agreement of what is being said (Budescu and Wallsten, 1985).

In summary, the problems with qualitative risk analyses concern both mathematics and psychological aspects of human decision making. The one fundamental issue that these factors unanimously cause is that the risk matrix and its ordinal scales potentially paints a misleading image of the risk landscape which makes it hard to draw any sound conclusions. As one Nixu employee puts it:

> The one crucial deficiency of the risk matrix is that it does not provide enough grounds for decision making. […] using the same matrix, you can reach completely different conclusions of how to prioritize risks. It is ambiguous in the sense that you cannot know what the remaining risks will be (Interviewee 2, 2019).

## 2.4 What are the gains of quantitative risk analysis?

Risk management is never perfect. Some might say, in defense of qualitative risk analyses, that no model will ever be able to provide complete answers. The future is uncertain, and fact is, that reality is far too complex to ever be modelled exactly (Freund and Jones, 2014). So, is it not better that we try to analyze our risks using qualitative models, than not trying at all? This is not something that this thesis will go against. However, we argue that there are better ways to approach risk management within cybersecurity and here we will tell you why.

The idea presented in this thesis is that quantitative risk analyses are more credible than qualitative ones. Let us begin with providing the definition of quantitative risk management that will be used here, inspired by the definition provided by Hewitt and Pam (2018) in the report *Qualitative Versus Quantitative Methods in Safety Risk Management*:

*Quantitative risk management is the process of assessing hazards using statistical techniques, such as Monte Carlo simulations, to quantify the risk associated with those hazards.*

To follow up on this definition, it is necessary to turn to quantitative measurement scales instead of qualitative ones since we now know that using mathematical functions on the latter is inconsistent. Quantitative risk management is based on continuous numerical values, both

for impact and likelihood, using data from a variety of resources such as historical incident data or input from people with knowledge about the business. Usually, the likelihood is rated in probabilistic terms and expressed as a percentage whereas impact is most commonly rated in monetary terms - two suitable estimators since both are on a ratio scale (ISO 27005, 2018). Let us look at what a quantitative risk management process may look like through a simple example:

**EXAMPLE 2**

Put yourself in the shoes of a risk analyst. You have been asked to help an organization prioritize risks and you have chosen to use a quantitative approach, instead of the commonly used qualitative model. The group assembled for the assessment has already identified four risks that the organization face: risk A, B, C and D, and you ask the participants to specify the likelihood of each risk happening within a year as a percentage and the expected impact in monetary terms if it were to occur. Hence, instead of asking the group to come up with ordinal scales towards which you can assess the risks, you give the participants the option to freely estimate the impact and likelihood from continuous ratio scales.

The participants start discussing possible values but do have some problems providing point estimates of the likelihood and impact of the risks. You try to the best of your ability to support them in the process, for example by suggesting points of reference and historical incident data. Eventually, the group has reached an agreement and you feel satisfied with the assessment. Since we are using ratio scales it is possible to make estimations based on mathematical operations and the risk level is therefore quantitatively calculated as $EL(X) = Likelihood(X) \cdot Impact(X)$. You summarize the result of the quantitative analysis in Table 1.

*Table 1. Example of results from a quantitative risk assessment*

| Event name | Likelihood (annual) | Impact (SEK) | Expected loss (SEK) |
|---|---|---|---|
| Risk A | 2.0 % | 400 000 | 8 000 |
| Risk B | 5.0 % | 5 000 000 | 250 000 |
| Risk C | 40.0 % | 10 000 000 | 4 000 000 |
| Risk D | 20.0 % | 15 000 000 | 3 000 000 |

You conclude the risk management process by identifying suitable treatments for the risks and by providing a summary of your findings to management. You are careful in your recommendations but explain that the results indicate that risk C seems to come with the highest expected loss if it remains untreated.

Example 2 provides a simple illustration of how a quantitative risk management process can be carried out. It is perhaps naïve in its expectations on the analysts' abilities to estimate precise values, but as we will show later in this thesis there are numerous ways in which the model can be improved and developed to capture the uncertainty of the assessor. A few such examples are to allow for range-estimations of the likelihood and impact and to introduce Monte Carlo simulations to generate a large number of possible scenarios and outcomes. These improvements will be the main theme of the rest of this thesis, but what these basic results show already in this stage is that mathematical operations and statistical methods actually can be implemented in a correct and consistent way if turning from ordinal to ratio scales.

Even though the quantitative approach has much to offer for the risk management community, it has not been warmly welcomed by everybody. In order to explain why we believe quantitative models are better suited for risk management, we will answer three central objections to quantitative risk modelling, often found in literature promoting qualitative methods:

1. Some risks are not possible to measure and quantify (Swedish Standard Institute, 2018, p. 49)

2. There is too little data to perform quantitative risk analysis (Wheeler, 2011)

3. Quantitative risk analyses are still only based on subjective judgements (Hubbard and Seiersen, 2016, p. 36)

Starting with objection number 1, it has been argued that some risks cannot be measured simply due to the fact that there is too much uncertainty surrounding the likelihood and impact of the event (Wheeler, 2011, p.40). According to Douglas Hubbard, author of the 2014 book *How to measure anything: Finding the value of intangibles in business*, this is a common misconception of risk and measurement. Hubbard argues that measurement should be looked upon as a probabilistic exercise and not, as many people seem to think, a process of providing *exact* answers (Hubbard, 2014, p.30). He states that "We use quantitative, probabilistic methods specifically *because* we lack perfect information, not in spite of it" (Hubbard and Seiersen, 2016, p.102). Scientists and experts alike know that certainty about real-world events is usually not possible to reach and that an amount of error is always unavoidable. Therefore, it is the *reduction* of uncertainty, not necessarily the elimination of it, that comprises the measurement (Hubbard, 2014, p.31). Jack Jones and Jack Freund, authors of the book *Measuring and managing information risk: A FAIR approach* from 2014, adds to these conclusions by stating the goal of measuring risks is to "reduce uncertainty to a useful level of precision" (Freund and Jones, 2014, p.77). Therefore, having even a single data point could count as a measure or quantification if your previous knowledge about the amount of risk associated with that event was nothing (Freund and Jones, 2014, p.77).

Objection number 2 is a close relative to objection number 1. The idea that there is usually too little data to perform a quantitative risk analysis is often presented in articles on the topic (see for example Wheeler, 2011, p.123; ISO 27000, p.49; The Open Group, 2013b, p.33). Arguments presented are along the lines that qualitative risk assessment is preferable since "data is inadequate" (Swedish Standard Institute, 2018, p.18) or that "sufficient data is not available" (Hewitt and Pham, 2018). Yet, the same speakers would have no problem estimating the likelihood as a 4 on a scale from 1 to 5 or as a medium-risk, which is not a very logical conclusion (D. Hubbard and Seiersen, 2016, p.38). As Hubbard puts it:

> Remember, if the primary concern about using probabilistic methods is the lack of data, then you also lack the data to use nonquantitative models (Hubbard and Seiersen, 2016, p. 38).

We now turn to the last stated objection towards quantitative risk management models, namely the idea that it would still only be experts making subjective judgments of the potential impacts of risks. This is partly true because even quantitative models rely on experts making judgements about likelihood and impact. The difference to the qualitative model, however, is that instead of using ordinal scales, such as low to high, quantitative models assess the actual quantities behind those scales (Hubbard and Seiersen, 2016, p.36). The advantage of such an approach is that we can transform the mental model that experts still use when reaching the conclusion medium, into a well-vetted formal model that can be critically reviewed and updated as new data is available (Freund and Jones, 2014, p.9).

In conclusion, this subsection has provided motivations for why we should turn to the quantitative risk analysis instead of the qualitative one. As has been shown, the quantitative analysis solves the issues that qualitative methods introduce by using ratio scales instead of ordinal ones and by assessing the actual numbers behind qualitative categories such as *likely* or *unlikely,* thus avoiding the illusion of communication. The cybersecurity community has tended to reject the quantitative model based on arguments that are not entirely factual, such as the impossibility to measure and quantify certain risks and the lack of data. Hubbard and Seiersen (2016, p. 96) argue that this aversion towards quantitative analyses also comes from an illogical comparison in which the quantitative assessment is often evaluated to some sort of infallible ideal that should produce exact results. Just like Hubbard and Seiersen, we believe that the quantitative model deserves more attention and that it should, instead of being compared to an unrealistically perfect model, be compared to the actual alternative: the qualitative analysis.

# 3. Related work

Quantitative approaches to risk management is not a new area of research. Disciplines such as insurance, credit risk, and business intelligence have used quantitative estimations as the go-to approach for many years and few of them would likely be returning to qualitative processes any time soon (D. Hubbard and Seiersen, 2016, p.108). In the cybersecurity community, however, quantitative risk management has just begun to make its entrance and in this section, we will present previous work made in the area.

## 3.1 Cybersecurity standards

A suitable starting point when discussing quantitative risk management models within cybersecurity is standards. Two of the most prominent standards for handling risks within cybersecurity are the previously mentioned publication *ISO/IEC 27005* from the International Organization for Standardization and the International Electrotechnical Commission (ISO 27005, 2018) and the *NIST special publication 800-30*, published by the American organization National Institute of Standards and Technology (NIST 800-30, 2012). In general terms, these standards have the same ambition to specify guidelines for cybersecurity risk management for different types of organizations. The main difference between them is that NIST SP 800-30 was developed mainly for managing risks relating to implementation and deployment of new systems within federal organizations in the U.S, whereas ISO 27005 is an international standard that is more imprecise in its recommendations. Both standards have become corner-stones in the process of managing risks within the cybersecurity community and several of the existing risk management models are built upon the ISO 27000 series and/or the NIST framework (Fenz *et al.*, 2014).

## 3.2 Risk management models

As previously stated, there are nowadays numerous risk management models available for use within the cybersecurity community (Dubois *et al.*, 2010). Some of these models are supported by a software whereas others are not, and the latter is therefore often referred to as paper-based models (Fenz *et al.*, 2014). Throughout the years, several organizations and researchers have made attempts to summarize, take stock of and compare existing models and frameworks, a few such examples being the European Union Agency for Network and Information Security, 2006, Kouns and Minoli, 2010, Gritzalis and Stavrou, 2018 and Dubois *et al.*, 2010. According to our experience, these comparisons often result in complex tables and analyses which are not always easy to comprehend or make use of. This experienced difficulty is reflected in the work of the global standards consortium The Open Group, who states that management selecting risk assessment methodologies are often not able to differentiate more effective methodologies from less effective ones, due to the complex risk methodology landscape and the difficulties in making comparisons (The Open Group, 2009).

To add to this adversity, only one of the previously mentioned inventory-works specifies whether a specific model is classified as either qualitative or quantitative (Gritzalis and Stavrou, 2018). It is likely that this seeming aversion towards classifying models as either quantitative or qualitative comes from the fact that it is often hard to draw a strict line between the two. As of today, several models include both qualitative and quantitative elements, a few such examples being MEHARI (Mihailescu, 2012), CSRM (Goel, Haddow and Kumar, 2018), MAGERIT, CORAS (Gritzalis and Stavrou, 2018), and COSO ERM (Bayuk, 2018). Other models, such as ISRAM (Karabacak and Sogukpinar, 2005) and Octave Allegro (Caralli *et al.*, 2007) claim to be quantitative, but according to our definition of a quantitative model (as stated in section *2.4 What are the gains of quantitative risk analysis?*) neither of these can be regarded as purely quantitative since they are both using numbered ordinal scales for risk estimation.

Yet another type of risk management method worthy of mentioning is the relative risk scores. Relative risk scores are used to measure and prioritize the severity of different computer security issues, by translating information given from the analyst to a numerical value. Examples of commonly used scoring systems within the cybersecurity community are the Common Vulnerability Scoring System (CWSS) (Forum of Incident Response and Security Teams [FIRST], 2019), the Common Weakness Scoring System (CWE) (The MITRE Corporation, 2014) and the Common Configuration Scoring System (CCSS) (Scarfone and Mell, 2010). Even though these are presented as quantitative methods, they too should be considered hybrid since they are really just adding up multiple ordinal scales to get an overall risk score. Just as in the case of the risk matrix, this is what should be considered improper maths (Hubbard, 2014, p.92).

## 3.3 Contributing authors

In this clearly complex environment, only a few authors have managed to create models that have become formally recognised within the cybersecurity community. Two such authors are Jack Jones and Jack Freund, who published the somewhat ground-breaking book *Measuring and Managing Information Risk: A FAIR Approach* in 2014. Here, Jones and Freund present their perspectives on the FAIR (Factor Analysis of Information Risk) methodology and a comprehensive risk ontology, where the notion of risk is decomposed into detailed mechanisms (Freund and Jones, 2014). The FAIR methodology is as of today considered to be the most complete, best analysed and well-defined methodology taxonomy available for cybersecurity purposes (The Open Group, 2010; Wheeler, 2011). Nevertheless, it has not yet reached a wide acceptance in the business much because of its complexity and perhaps overly comprehensive treatment of the risk problem (Wheeler, 2011, p.291; The Open Group, 2013a).

Another well-renowned author in the field of quantitative risk management is Douglas Hubbard. Together with the cybersecurity expert Richard Seiersen, he authored the pioneering book *How to measure anything in cybersecurity risk*, published in 2016. As the

title suggests, their main argument is that everything is measurable and that the single most important measurement in cybersecurity risk management is to measure how well the risk assessment methods themselves work. If you are using a risk management method that does not work, or even worse: a method that you think works, but produce inaccurate results, Hubbard and Seiersen argue that you could actually be worse off than if you did not perform any risk analysis at all (Hubbard and Seiersen, 2016, p.56). The authors oppose the common objection towards quantitative assessment as complex and impossible due to lack of data, by describing that even simple quantitative risk assessments have been scientifically proven to provide more accurate results than qualitative ones (Hubbard and Seiersen, 2016, p.95).

Whereas Hubbard and Seiersen raise the argument that the most important part of risk management is to measure how well the risk assessment method itself works, other authors present different ideas of what is the most fundamental part of risk management. Adolph Cecula (1985) and Andrew Baze (2014), both put forward the somewhat drastic argument that risk management modelling should be abandoned. Instead of spending time on analysing potential risks, their suggestion is that organizations should simply focus on implementing baseline security requirements on all systems in the organization, such as the CIS critical security controls (Center for Internet Security [CIS], 2018), since it is a more time-efficient and less costly way to handle risks. Their argument is clamped down by Rebecca Slayton in her article *Measuring Risk: Computer Security Metrics, Automation, and Learning* from 2015, where she claims that the most important part of risk management is not to measure the functionality of the risk assessment method, nor to implement baseline security requirements. Instead, her argument is that it is the *learning* that can come from risk assessments which is the central part of risk management. By conducting risk assessments, employees and other stakeholders will generate and spread awareness of cyber risks threatening the organization as well as improving their knowledge about computer security hazards, and that is according to Slayton, the most important part of the risk management process (Slayton, 2015).

# 4. Methodology

This project has been carried out over 20 weeks and was initialized with a brief literature study to gain a basic understanding of risk management in cybersecurity. The brief literature study was followed by the three main phases of the project: information retrieval, model development, and testing/reviewing. Figure 3 provides a quick overview of how these methodological processes relate to one another and how we have worked with them at different stages throughout the project.

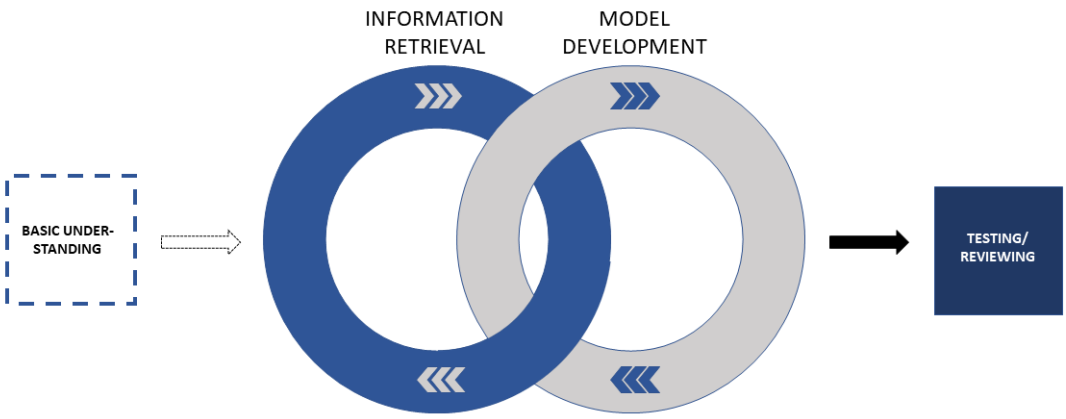



*Figure 3. The methodological process of the project.*

As the illustration aims to demonstrate, our risk management model has been created using a combined iterative and linear, waterfall, approach. The first step in the process was to gain a basic understanding of risk management in cybersecurity. This was done by reading into the subject, skimming several articles and books on the topic and by discussing the phenomena in broader terms with cybersecurity specialists at Nixu. Having established a solid knowledge base, the project entered an iterative stage where information about risk management models was collected while we started sketching for and designing our model. Hence, the model was iteratively created and improved while our knowledge about cybersecurity risk management increased. In the final stage of the project, we once again entered a more linear phase in which we tested our model on one of Nixu's customers during a workshop. Optimally, this third phase of testing would have been included in the iterative process as well so that the results from the evaluation were used to update and improve the model even further. Due to time constraints the implementation of the proposals and ideas raised during the testing phase have not been realised in the current model, but are outlined in section *9.2 Future work*.

Each of the three main phases: information retrieval, model development, and testing/reviewing have contained its own subprocesses and challenges. In this section, we will outline how we have methodologically approached each of them.

## 4.1 Information retrieval

The information used in this study has been collected from two main types of sources: available literature on cybersecurity risk management and cybersecurity consultants working with risk management at Nixu. We will describe how we have retrieved information from each of these two types of sources below.

### 4.1.1 Literature study

As stated in Jan-Axels Kyléns book *Att få svar: intervju, enkät, observation* (Finding answers: interviews, surveys, and observations), reading is probably the most common way of collecting information for academic research (Kylén, 2004, p.3). For this thesis, we have conducted a thorough literature study on material varying from books and academic papers to business standards and online resources. The material has been studied for different purposes such as understanding the difference between qualitative and quantitative methods, establishing requirements for risk management models and for finding inspiration from already existing cybersecurity risk management models. The relevant material studied in this project can be found in the reference list at the end of this paper.

One book that deserves to be mentioned specifically is *How to measure anything in cybersecurity risk* by Douglas Hubbard and Richard Seiersen. The book, which was published in 2016, has become somewhat a game-changer in the field of cybersecurity risk management (Winterfeld, 2016) and we have gained a lot of inspiration from Hubbard and Seiersen's extensive descriptions of quantitative risk modelling. Apart from reading it ourselves, we have also taken part in a book club covering Hubbard and Seiersen's book. The book club was arranged by Nixu and SIG Security (a Swedish association of professionals within the cybersecurity field) and sessions were held practically every third week for three months. Other organizations interested in cybersecurity risk management were also invited to take part and we learned a lot by listening to cybersecurity professionals discussing the possibilities and drawbacks of Hubbard and Seiersen's work.

### 4.1.2 Interviews and survey

To capture cybersecurity professionals' perceptions and ideas of factors that contribute to a successful risk management model, we conducted three interviews and sent out a survey to cybersecurity consultants working at Nixu. The three interviews were all carried out on the 19th of February 2019 and each session lasted for about one hour. We also sent out an online survey to twelve consultants working at Nixu at the end of February and received ten answers within a week.

#### 4.1.2.1 Methodological aspects of the interview

The interviews were to a large extent unstructured, meaning that we had prepared questions before the sitting but kept the discussions open to capture interesting themes and thoughts that the interviewees brought up spontaneously (Kylén, 2004, p.19). Both of us participated

in the sessions, taking a turn on acting as the interviewer and taking notes. The three interviewees selected to take part were all entitled cybersecurity consultant. The reason why these three employees were chosen as interview subjects were that they had solid experience of working with cybersecurity risk management at Nixu. The list of questions asked during the interview can be found in *Appendix A.*

To analyse the collected material from the interviews, we used the methodology *content analysis*. The reason we chose to use this method was that it is an established research technique for making valid inferences from texts and other types of communications, such as interviews and observations (Drisko and Maschi, 2015). Content analysis can be carried out in various ways, but it usually contains the following four steps: 1. Understanding the data, 2. Finding so-called recording units, 3. Coding the recording units and 4. Formulate themes that emerge from the coded recording units (Drisko and Maschi, 2015).

The first step of the process was completed by carefully reading through the notes from the interviews and discussing potential ambiguities. The second step, finding recording units, deserves a more elaborate explanation. Recording units are passages of text that the analyst finds specifically meaningful or segments of data that convey certain meanings of interest (Drisko and Maschi, 2015). Examples of such recording units in our analysis were sections where the interviewees mentioned factors that contribute to a successful risk management process or expressed needs that the current processes do not fulfil. Statements such as “The most critical factor of success is to set the scope of analysis” and “… communication of risks is hard” were among those approximately 20 recording units found.

Moving on to the third step, we assigned a code name to each of the recording units. As Drisko and Maschi (2015) points out in their book *Content Analysis* from 2015, the process of coding recording units is often complex as it requires many interpretive decisions of the researchers. We tried to the best of our ability to inductively assign accurate code names to the recording units by independently reviewing the same material and then comparing our suggested coding. An example of the results of our coding process is the record units “How to prioritize risks is unclear in the risk matrix” and “Risk management is supposed to help you with prioritization”, which were both coded as *prioritization of risks*.

The last step in the content analysis is to formulate themes from the coded recording units. Since the purpose of the interviews was to find factors that contribute to successful risk management processes, our ambition in this stage was to translate the coding into well-formulated needs among the users. A few examples of such needs were that the model should be *time-efficient* and that it should allow for *clear communication of results.*

Having provided this methodological basis for how we carried out the interviews and analysed the collected material, a detailed description of the content of the interviews will be given in section *6.1.1 Review of interviews.*

#### 4.1.2.2 Methodological aspects of the survey

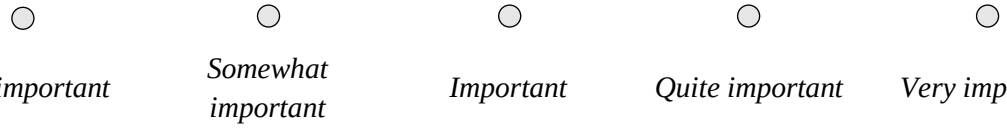
In addition to the interviews, we sent out an online survey to information security consultants working at Nixu. The survey contained six scale-questions aimed to capture the importance of different factors of risk management. The survey also posed two concluding questions where the respondent could provide his or her own suggestions of factors contributing to successful risk management processes and add general comments about the survey. As previously stated, ten Nixu-employees answered the survey and we recorded their responses anonymously. The survey can be found in *Appendix B.*

The six questions in the survey were constructed as Likert-type scales, named after the American phycologist Rensis Likert. The basis of the Likert-scale technique is that the respondent is asked to state how much he or she agrees with a certain statement on a scale with an equal amount of positive and negative possible answers. The range of possible values aims to capture the intensity of the respondent's feelings for a given statement (Hagevi and Viscovi, 2016, p.108). Each question in the survey started with the following passage: "How important is it to you that the risk management model…", followed by a statement concerning a specific factor of risk management modelling. The six factors that were studied in the survey were:

- Time-efficiency when it comes to implementation
- Time-efficiency when it comes to understanding of the risk management model
- The model's ability to handle "soft" aspects of risk (such as reputation and competitive advantage)
- The model's ability to provide detailed results (such as tables or graphs)
- Easiness of communication to the whole organization
- Easiness of communication to management

The reason why these factors were considered interesting to study is that they were the ones that were most commonly brought up as deficiencies of current qualitative risk management processes in initial discussions with Nixu employees. Moreover, these factors were motivated by the fact that they are often mentioned as necessary features of successful risk management processes in the literature (more about this in section *6 Model requirements*).

Each of the six scale-questions offered the following five-levelled possible answers, and the respondent was asked to choose one of them:




It may seem contradictory to use a qualitative assessment method in a study strictly promoting the use of quantitative scales, and we would, therefore, like to clarify our choice of research methodology. First of all, the purpose of our survey was to capture the viewpoints of cybersecurity professionals regarding success factors for risk management models. According to Hagevi and Viscovi, Likert-scales are as of today one of the most common research methodologies for retrieving this kind of information (Hagevi and Viscovi, 2016, p.108). Secondly, the results of our survey have *not* been used to make statistical inferences or draw mathematical conclusions. Our sole ambition was to gain indications of which factors should be prioritized in our developed model.

As stated by Hagevi and Viscovi (2016, p.176) digital surveys are superior compared to paper-based ones since they are cheaper, more precise and less time-consuming. The choice was therefore made to create our survey using the online tool Kurt, provided by Uppsala University. The survey was emailed to twelve Nixu employees, who could access and answer the survey through a web-link. Since the responses were collected anonymously and the content of the survey did not concern any information that should be regarded confidential, we considered it judicious to use an online survey, instead of a perhaps more secure paper-based one.

Having provided this methodological basis for how we created and conducted the survey, a detailed description of the results will be given in section *6.1.2 Review of the survey.*

## 4.2 Model development

There are several aspects to consider when developing a risk management model. One such obvious feature is to make sure that the users of the model find it useful and applicable. To make sure that our developed model reached the needs of the users and the cybersecurity community we decided to base it on a number of requirements. These requirements were collected from three types of sources: from Nixu consultants working with risk management (through the previously described interviews and the survey), from the literature and from our own perspectives on risk management modelling. The requirements were not only used to guide us in the process of developing a more accurate and efficient risk management model but also to evaluate whether our developed risk management model really was an improvement compared to current practices. The established requirements will be outlined in section *6 Model requirements.*

Another relevant aspect of risk management modelling is that the model is suitable for the industry. To meet this criterion we decided to base our model on an already existing risk management framework, namely the ISO 27005 cybersecurity risk management process, introduced in section *2.1 What is cybersecurity risk management?* (see Figure 1). Since ISO must be considered a serious actor on the global arena, and since their standard 27005 has gained wide acceptance in the cybersecurity industry, we considered it an appropriate choice of springboard. As demonstrated in Figure 4, we chose to limit the scope of development to three of the eight mentioned activities in the ISO-framework: *risk analysis*, *risk evaluation* and *risk communication and consultation.* Throughout the thesis, we have chosen to refer to these three activities as the *core activities.*

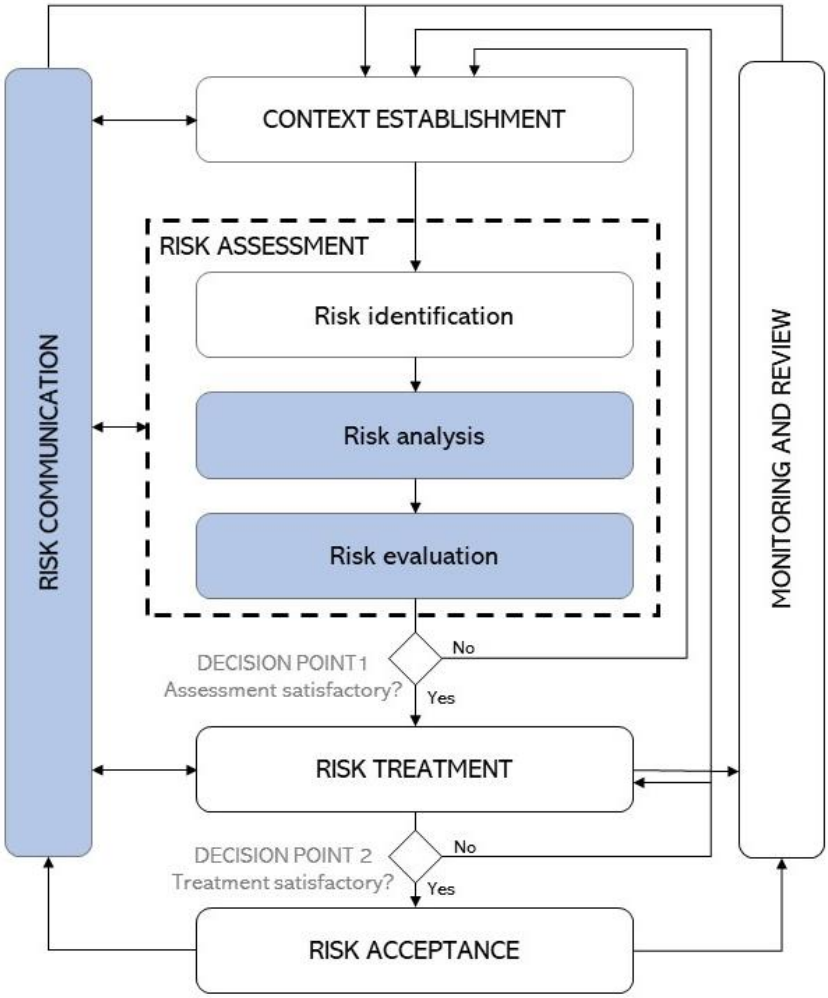



*Figure 4. Core activities of the MaRiQ model.*

The motivation behind our focus on these core activities was three-folded. First, it is the risk analysis that can be classified as either quantitative or qualitative – hence, it was a necessary activity to consider given our goal of creating a quantitative risk management model. Second, risk evaluation is closely connected to the risk analysis since the evaluation is based on the established risk level - thus, it was a logical addition to the core activities. Third, risk communication is a necessary prolongation of the risk assessment since an assessment that cannot easily be communicated to management and/or the rest of the organization is not very

useful. Therefore, we also chose to add the process of communication to our core activities. During our model development, we have been focusing on furthering communication in terms of visualization of results.

Our developed model consists of two parts: a paper-based model-description that outlines how the activities in our model should be carried out and a digital tool, that supports the core activities. The tool was created using Microsoft Excel, a spreadsheet software developed by Microsoft that features calculations, graphing tools and the programming language Visual Basic for Applications (VBA) (Microsoft, 2019). The main reason why we chose to work with Excel and VBA is that Excel is one of the most widely used spreadsheets applications in businesses today (Techstore, 2013). This general knowledge of Excel makes us believe that it is easier for potential users of our model to implement and understand the tool than if we had chosen to use any other software candidate such as Python, R or JavaScript. The developed model-description will be further outlined in section *8.1 Description of the MaRiQ Model* and the associated tool in section *8.2 Description of the MaRiQ* Tool.

In summary, our model is developed based on the ISO 27005 framework and on established requirements for the risk management process. The model consists of two parts: a paper-based model-description and a digital tool, that supports the stated core-activities. Our model is intended to hook on to the already existing ISO-framework, which means that non-core activities, such as risk identification and risk treatment, are still just as necessary to carry out but that our model-description and tool will only support the risk analysis, risk evaluation, and risk communication. The way the core activities have been developed will be presented in section *7 Core activities*.

## 4.3 Testing/reviewing

To make sure that our model and its accompanying tool was functioning according to its purposes, we tested and reviewed the model in two ways. First, we continuously validated the tool by running tests in Excel to make sure that there were no defects or other unwanted issues. Secondly, we tested the model in its entirety through a client-case with one of Nixu's customers. Below, we will explain each of these testing phases more thoroughly.

### 4.3.1 Tool validation

As previously mentioned, the tool was created using Microsoft Excel and the VBA programming language. During the development, we carefully tried each function – in Excel called *subprocess* – by printing out error messages, trying different corner cases and by always keeping four eyes on the code. A few examples of errors that we fixed in our validation process were erroneous cell references, miscalculated formulas and reprinted results.

### 4.3.2 Client-case

To test our model in its entirety, we invited one of Nixu's customers to take part in a real-life scenario risk management workshop. The workshop was conducted during two half-days, one the 15th of May and the other on the 17th of May. The customer taking part in the assessment was active in the banking industry and had previous experience of performing qualitative risk analyses.

The working group that was established for the task consisted of nine people: five employees at the customer, two Nixu-employees (our supervisors) and the two authors of this thesis. Our roles were made clear during the first session: the customer-employees provided expertise regarding the customer's organizational and financial context, the Nixu-employees provided expertise with regards to cybersecurity hazards and we were the leaders of the workshop providing information of how the risk management process should be carried out.

During the first workshop session, on the 15th of May, we helped the working group carry out the analysis using our developed model with support from the tool. The results achieved were left with the working group to ponder on to the next session. During the following session, the 17th of May, we asked the working group to reflect on the risk management process we had carried out two days earlier. To capture their thoughts and ideas in an orderly fashion, we had prepared evaluative questions, found in *Appendix C*, that were asked during the group discussions. Our ambition was to understand the strength and weaknesses of our model and to see if the group found it useful in comparison to current qualitative practices.

A thorough description of the client-case procedure and results will be presented in section *8.3 Review of client-case.*

# 5. Statistical aspects of risk management modelling

One absolutely necessary ingredient in quantitative risk management modelling is statistics. In our developed risk management model, we have used several statistical techniques to achieve accurate and reliable results. This section is dedicated to describing the theoretical setting of these statistical aspects. We start off by providing a brief outline of probability distribution functions, followed by a description of commonly used distributions in quantitative risk analyses. Thereafter, we will discuss the probabilistic terms uncertainty and variability as well as describing the random sampling method Monte Carlo and touching upon Bayesian approaches to statistical analyses. How these concepts relate and apply to our model will be described and motivated and in section *8.2.2 Statistical considerations of the MaRiQ tool.*

## 5.1 Probability distribution functions

A probability distribution function is a function that is used to define a particular probability distribution. There are two fundamental probability distribution functions for continuous variables: the *cumulative distribution function* (cdf) and the *probability density function* (pdf). These are mathematically defined as in Equation 2 and 3:

- The cdf, *F(x)*, is defined as the probability P that a variable *X* is less than or equal to *x*, written as:

$$F(x) = P(X \leq x) \tag{2}$$

- The pdf, *f(x)*, is defined as the gradient of the cumulative distribution function, i.e.

$$f(x) = \frac{d}{dx}F(x) \tag{3}$$

There is no probability directly associated with specific values of *x* in the pdf due to the infinite number of values. However, the area under the function – the integrated pdf – must equal 1 since it is the sum of all probabilities (Vose, 2008, p.115-118). Hence, the pdf represents how probable different outcomes are *in relation* to each other rather than specific probabilities. Figure 5 illustrates the relationship between the pdf and the cdf for a normal distribution.

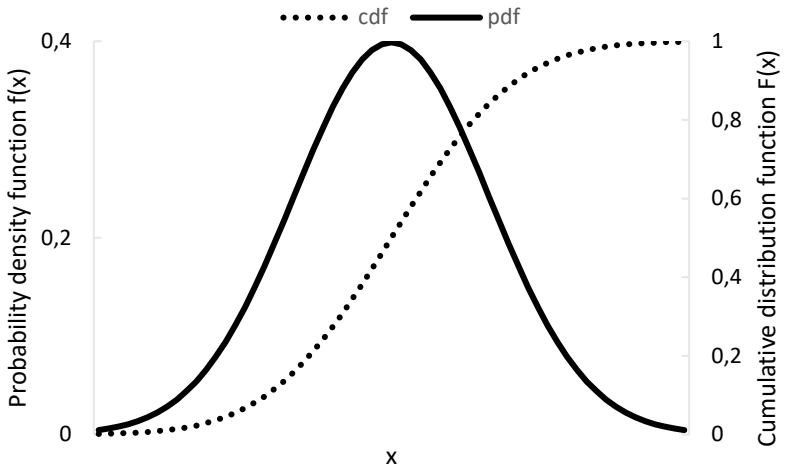



*Figure 5. The probability density function and cumulative distribution function for a normal distribution.*

An important property of the pdf is that it can be used to compute a *confidence interval*. A confidence interval is a type of interval estimate, that contains a range of potential values associated with a so-called confidence level. The confidence level describes the level of confidence that the true value lies within the specified range. Commonly used confidence levels are 95% and 90 % (Alm and Britton, 2008, p.299). By using a confidence interval, we can express the degree to which we are certain that the true value actually lies within a range. For example, a 90 % confidence interval indicates that there is a 90 % chance that the interval contains the correct answer (Alm and Britton, 2008).

## 5.2 Distributions

There exist numerous distributions in the world of statistics. For the purposes of this thesis, we have chosen to focus on only a few of these, applicable to modelling risks. The five presented distributions are the uniform, normal, lognormal, triangular and beta distribution.

### 5.2.1 Uniform distribution

The historically first studied probabilities were uniformly distributed. In a uniform distribution, all possible outcomes have the same probability (Alm and Britton, 2008, p. 14). The distribution is defined by the two parameters *a* and *b*, which are the maximum and minimum values. All values outside *a* and *b* have the probability zero (Vose, 2008, p.404). It follows from the definitions of the probability density function and the uniform distribution that the probability density for the possible outcomes is one divided with the length of the range of possible values. The probability density function is shown in Figure 6.

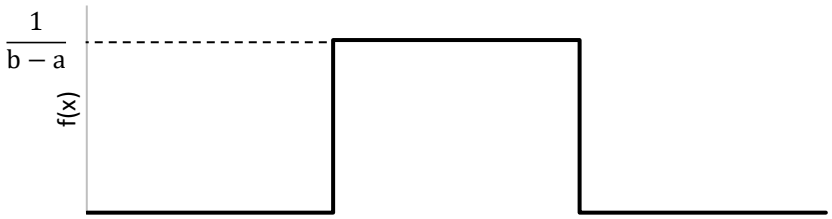



*Figure 6. Probability density function for uniform distribution with minimum value a and maximum value b.*

The uniform distribution is suitable to use when little is known about the parameters of the distribution. However, it can be unrealistic in some cases that the probability falls to zero at the minimum and maximum value (Vose, 2008, p.404-405).

### 5.2.2 Normal distribution

Perhaps the most well-known distribution is the normal distribution. One of the reasons it is considered so important is that the sum of several random variables is almost always normally distributed. The normal distribution has a bell-shape and is defined by its parameters μ (expected value) and $\sigma^2$ (standard deviation) (Alm and Britton, 2008, p.100-102). Figure 7 shows the probability density function for a normal distribution with μ=0 and $\sigma^2$=1.

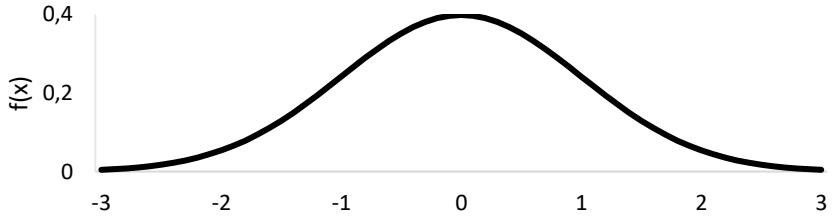



*Figure 7. Probability density function for normal distribution with $\mu$=0 and $\sigma^2$=1.*

Many naturally occurring variables can be well approximated by normal distributions. In addition, it is suitable to use when it is equally probable to observe a result below the mean as above due to its symmetric shape (Hubbard and Seiersen, 2016, p. 241).

### 5.2.3 Lognormal distribution

A random continuous variable Y is lognormally distributed with the parameters μ and $\sigma^2$ if the natural logarithm of Y is normally distributed, that is: ln Y ~ N (μ, $\sigma^2$). The parameters μ and σ are the expected value and variance respectively for the normal distribution, not for the lognormal distribution (Alm and Britton, 2008, p. 111). Figure 8 shows the probability density function for a lognormal distribution with parameters μ=0 and $\sigma^2$=1.

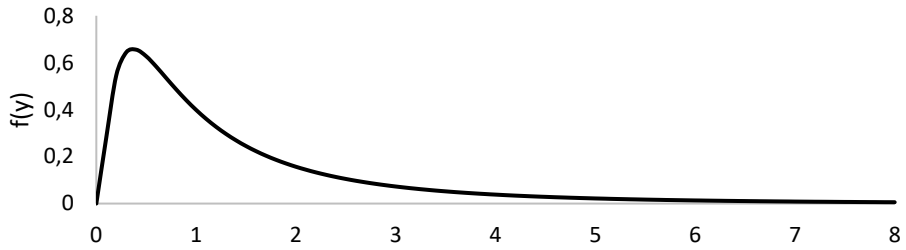



*Figure 8. Probability density function for a lognormal continuous random variable Y with parameters μ=0 and $\sigma^2$=1.*

A lognormal distribution only allows for positive values and has a right tail, which breeds for the possibility of rare extreme values (Vose, 2008, p.658). These characteristics make the lognormal distribution a realistic representation of probabilities of various amounts of loss (Hubbard, 2014, p.41).

### 5.2.4 Triangular distribution

The triangular distribution has, as the name indicates, the shape of a triangle and is defined by its minimum (a), most likely (b) and maximum (c) values (Vose, 2008, p.403). The minimum and maximum values are absolute limits, meaning that there is no chance of generating a value outside these bounds. The most likely value is located between the maximum and minimum value and determines where the peak of the triangle is located, as shown in Figure 9 (Hubbard and Seiersen, 2016, p. 239-240).

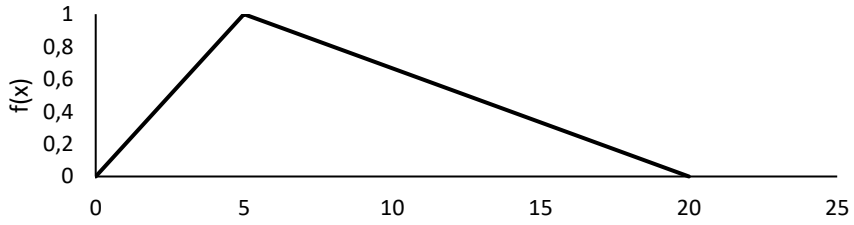



*Figure 9. Probability density function for a triangular distribution with a=0, b=5 and c=20.*

The triangle distribution is commonly used to model expert opinion and is considered appropriate when little is known about the parameters outside the minimum, most likely and maximum value. However, the straight lines and clearly defined bounds somehow contradict this uncertainty and can, therefore, be claimed to be unrealistic (Vose, 2008, p.403).

### 5.2.5 Beta distribution

The beta distribution is defined by its parameters α and β. Depending on the values of these parameters, the distribution obtains different shapes. For example, if α and β are both equal to

one, the beta distribution is a uniform distribution. Moreover, the beta distribution is only defined between zero and one (Alm and Britton, 2008, p.114-115). Figure 10 shows how the shape of the beta probability density function changes for different parameter values.

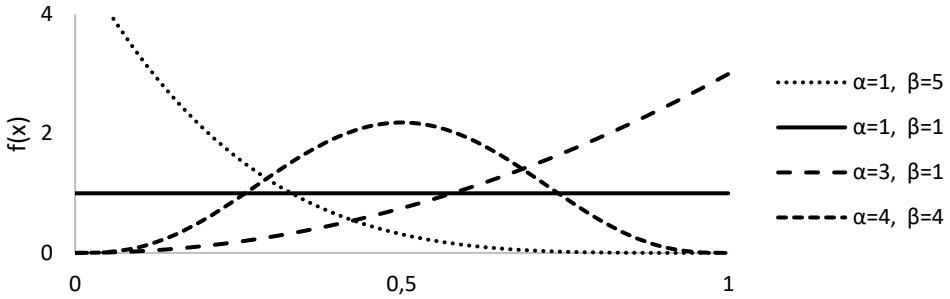



*Figure 10. Beta probability density function for four different combinations of parameter values.*

The beta distribution is commonly used to model continuous variables that take values between zero and one (Alm and Britton, 2008, p.115). Both fractions and probabilities have this property and the description of them is one of the main uses of the beta distribution. Another useful feature of the beta distribution as described (and illustrated in Figure 10) is the fact that it can take on a wide range of shapes over any finite range (Vose, 2008, p. 600).

## 5.3 Statistical measures

One way to analyse and compare distributions is to use statistical measures. These statistical measures can be categorized into three groups: measures of location, measures of spread and measures of shape. Below, each of these groups is outlined as described by Vose (2008, p.90-95).

- *Measures of location* describe the centre of the data distribution, also known as central tendency. The three most common measures are mode, mean and median. The mode is the value most likely to occur, the mean is the average of the output values, sometimes referred to as the expected value, and the median is the middle value of the output values. These concepts are graphically presented in Figure 11.

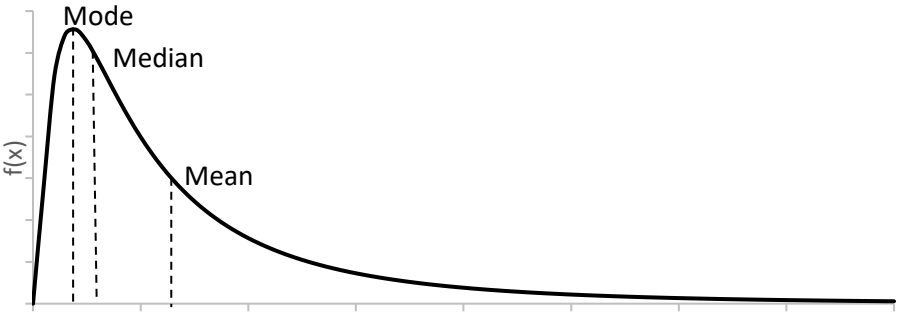



*Figure 11. Illustration of mode, median and mean in a probability density function.*

- *Measures of spread* describe the width of the distribution. Common statistical measures are variance, standard deviation, and range. The variance is essentially calculated by taking the average of squared distance between all output values and the mean. The standard deviation is the square root of the variance and the range is simply the difference between the maximum output value and the minimum.

- *Measure of the shape* aims to describe the appearance of the distribution, for example, if it has a tail or a peak. Example of measures describing what the distribution looks like is skewness and kurtosis.

## 5.4 Variability and uncertainty

No matter the distribution used, or how it is evaluated using statistical measures, there will always be some form of imprecision in human estimates of future events. In theory, there are two elements contributing to this imprecision: *variability* and *uncertainty*. Variability, sometimes called stochastic variability, is a function of the system itself and refers to its natural randomness. Hence, variability can only be reduced by changing the very system. The other component of our inability to precise predictions is *uncertainty*. In contrast to variability, uncertainty can sometimes be reduced by further studies and measurements since it relates to the estimators' lack of knowledge. Whereas the variability is a function of the system, uncertainty is a function of the assessor and is therefore sometimes referred to as degree of belief. The combination of variability and uncertainty is called *total uncertainty* (Vose, 2008, p. 47-54).

In a risk management model, variability and uncertainty can be evaluated separately. One advantage of such a separation is that we know what component of the output distribution is due to variability and what is caused by uncertainty. By doing so, it is easier to decide if we want to improve the measures even further or if the total uncertainty is simply due to the stochastic behaviour of the system. Although this separation can be useful, the additional time and effort to do so must be weight against the value of the results. Simulating risks without separating variability from uncertainty will also produce reasonable estimates of the total uncertainty of the output (Vose, 2008, p. 47-54).

## 5.5 Monte Carlo Simulations

A notable advantage of using quantitative approaches to risk management is that it is possible to statistically simulate the outcome of the estimated risks. Monte Carlo is one such sampling technique, used to produce hundreds or even thousands of scenarios. These scenarios are randomly sampled from probability distributions. When performing a large number of simulations, the sampled values reproduce the shape of the probability distribution from which it is sampled. However, it is important to be aware of the fact that the replication of the input distribution is heavily dependent on a very large number of simulations. Otherwise -

and this is one of the most common objections against Monte Carlo simulations - it can be considered nothing more than an approximation technique (Vose, 2008, p.45-59).

The random numbers used in the Monte Carlo method are computer generated. Since the computer creates random numbers by using deterministic algorithms, thus mimicking the property of real random numbers, the computer-generated random numbers are called pseudo-random numbers (Rychlik and Rydén, 2006, p.54)

Compared to other calculations methods, such as exact algebraic solutions and numerical approximations, Monte Carlo simulations offer many advantages. One such advantage is that there are several commercially available software to automate the simulations. The fact that the software performs the computations is one of the reasons why the model can easily be changed, updated, and compared to previous results. From a more mathematical perspective, Monte Carlo is advantageous since it only requires a basic level of mathematical knowledge while still enabling complex developments with no extra difficulty (Vose, 2008, p.45).

The Monte Carlo sampling method is based on random sampling from input distributions. We introduce the distribution of an input variable *x*. As described in section *5.1 Probability distribution functions*, the cumulative distribution function, *F(x)*, is defined as the probability P that the variable X will be less than or equal to *x*, written as:

$$F(x) = P(X \leq x) \tag{4}$$

By definition, the values of *F(x)* ranges from 0 to 1. Instead of evaluating the value of F(x), we can look at the inverse of Equation 4. That is, for a given value of *F(x)*, what is the value of *x*? This way of looking at Equation 4 in the opposite direction is defined in Equation 5.

$$G\big(F(x)\big) = x \tag{5}$$

It is the inverse function, *G(F(x))*, that is used when generating random samples from input distributions in Monte Carlo simulations. To use the inverse function, a random number *r* is generated from a uniform distribution with minimum value 0 and maximum value 1 (i.e. $r \sim U(0,1)$). This value, *r*, is then inserted into the inverse function instead of F(x), which can be described as Equation 6.

$$G(r) = x \tag{6}$$

The concepts of the cumulative distribution function, *F(x)*, and the inverse cumulative distribution function are graphically presented in Figure 12 (Vose, 2008, p.45-59).

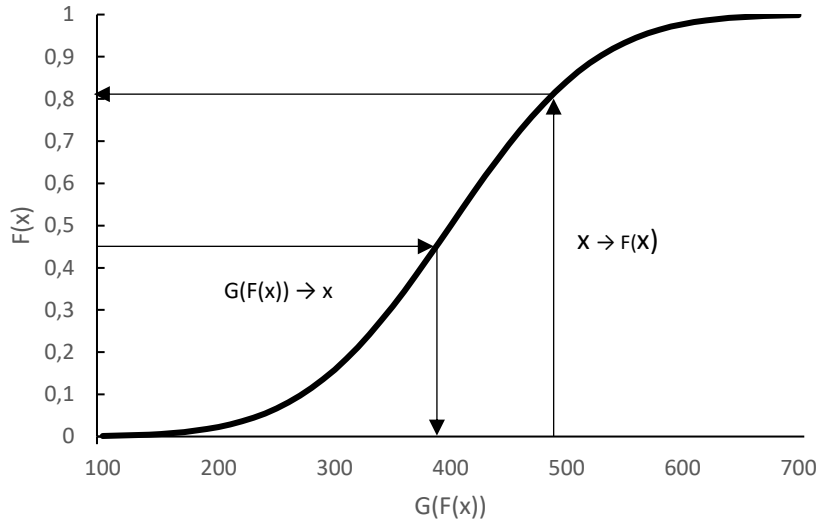



*Figure 12. How the cumulative distribution function, F(x), and its inverse, G(F(x)), relate to each other*.

## 5.6 Bayesian approaches to risk management

As described in section *2.4 What are the gains of quantitative risk analysis?* the term measurement is in this thesis treated as a reduction of uncertainty. Embedded in this definition is the assumption that there is some form of prior state of uncertainty that can be reduced. To measure the change in uncertainty it is common to use probabilities (Hubbard and Seiersen, 2016, p.24).

Since it is the observer making the probabilistic estimates, the term probability refers to the state of uncertainty of the observer, and not of the object being observed. Therefore, this view of probability is sometimes called the *subjectivist* interpretation, or in more theoretical terms: the Bayesian approach. Thomas Bayes was a British mathematician who came up with a simple, yet revolutionizing formula that became one of the world's most famous statistical measures. Bayes' theorem, as it is called, is formulated in Equation 7 (Rychlik and Rydén, 2006, p.22-24).

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \qquad (7)$$

The theorem states that using prior probabilities, we can update these prior estimates and retrieve a posterior probability after gaining new knowledge. This realization is important for decision making since, in reality, it is nearly impossible to make a decision without using a prior uncertainty, even though we rarely explicitly state these probabilities (Hubbard and Seiersen, 2016, p.25)

# 6. Model requirements

So far, we have provided an introduction to the field of quantitative risk management (sections *2 Background* and *3 Related work*) and an explanation of the formalities needed to construct our risk management model (sections *4 Methodology* and *5 Statistical aspects of risk management modelling*). Now, it is time to turn to the third part of this thesis, namely the results of our work. As stated in section *1.2 Disposition,* this third part consists of three sections: model requirements, model framework and a description of the model itself. This is the first of those three sections, aiming to clarify the requirements of the model and how these have been collected.

To build our model on stable grounds, we decided to put together a list of requirements that specifies characteristics of an accurate and successful risk management model as presented in section *4.2 Model development*. The requirements presented here have been collected from three types of sources: from information security consultants working at Nixu (referred to as *the users*), from available cybersecurity risk management literature and from our own perspectives on the project. Here, we will outline the requirements from each of these sources in detail. At the end of this section, a total of eight requirements will have been presented and motivated as of why they constitute the basis of our developed cybersecurity risk management model.

## 6.1 Input from the users

In order to understand the users' requirements and needs, we conducted three interviews with information security consultants and sent out a survey to cybersecurity specialists working at Nixu. All participants had previous experience of working with risk management, both internally and for external customers. Below is an outline of the major findings from these data collections, starting with the results from the interviews.

### 6.1.1 Review of interviews

As presented in section *4.1.2 Interviews and survey*, the interviews we conducted were unstructured and contained twelve loosely formulated questions, available in *Appendix A.* From the interviews we found that as of today, Nixu consultants are mainly using a qualitative approach to risk management where risks are assessed according to the ISO 27000 series. Two of the interviewed consultants were convinced that moving towards more quantitative approaches is necessary to improve the process, whereas one was more sceptical towards the promises of quantitative modelling. This consultant believed, however, that *if* data was readily available, quantitative models would be preferable.

During the content analysis of the collected material, as described in section *4.1.2.1 Methodological aspects of the interview*, ten themes emerged as mentioned by the interviewees. The first of these themes was *communication.* All consultants highlighted that

communication is a vital part of risk management and that the risk matrix is to a large extent still used simply due to the fact that it is easy to communicate and visualize. As one interviewee put it:

> The heat map is concrete, and visualisation is very important. In the end, it is the visualisation that makes the big difference (Interviewee 3, 2019).

The second most commonly mentioned theme was *difficulties in estimating impact and likelihood*. All of the consultants desired more support when it comes to finding accurate estimates, both for impact and likelihood. The interviewees mentioned that more data could be one solution to the problem, but that it is also necessary to have better methods for estimation. Secondary losses of risk, such as reputation and competitive advantage, were mentioned as especially difficult to estimate and the interviewees stated that they would like to get more support from the model when it comes to estimating these.

Thirdly, *prioritization of risks* was mentioned as a prevalent issue. The consultants stated that it is unclear how to prioritize risks in their current processes since the risk matrix does not state which of the red risks are most critical. It was, therefore, desired that the developed model would help with these prioritizations, by providing answers to which risks are most critical and by giving explanations to why these risks are more relevant.

Two other themes that were mentioned in the interviews were *competent personnel* and *review of the process.* When discussing competent personnel, the interviewees mentioned that knowledgeable analyst leaders and experienced participants who understand the business are crucial parts of risk management. Review was also considered a relevant ingredient to learn from previous experiences and preferably make use of incident history. One interviewee mentioned that an advantage of using the quantitative approach instead of the qualitative one is that:

> …if you have quantitative results you can easily change the monetary value, which you cannot do in a qualitative analysis (Interviewee 2, 2019).

*Scientific grounds* was a sixth theme that was mentioned during the interviews. The consultants requested that the developed model should be more statistically reliable in the sense that the results should be less dependent on the person or group carrying out the analysis. One consultant expressed this dilemma in the following way:

> One disadvantage [of the qualitative model] is that it is unscientific. If we have one group of analysts in one room analysing the risks, and another group performing the same analysis, we will end up with completely different results, even though we are analysing the same object (Interviewee 1, 2019).

Another interviewee mentioned that the qualitative approach provides more room for expert mistakes, since it entails less, or no, discussion about quantitative estimates.

Four themes that were not as frequently mentioned as the previous ones, but still touched upon in all interviews were that the model should be time-efficient, easy to understand, support the risk identification process and enable accurate scoping. *Time-efficiency* was

presented as a relevant feature of risk management in cybersecurity since customers are often busy with their own core business and usually do not have much time to spend on risk management. As one Nixu consultant put it:

> We cannot usually demand more time [from the customer], instead, we must find models that are more efficient and take time into consideration (Interviewee 1, 2019).

In relation to time-constraints, a discussion of the model's ability to *easily be understood* was brought up. One of the stated advantages of the current qualitative process was that it is easy to understand, both for the customers and the analyst, which makes it more efficient to put into practice. This simplicity in use was therefore also requested for the developed, quantitative model.

The theme *support in the risk identification process* was also brought up by the interviewees, and the consultants requested that the developed model should help to identify accurate and plausible risks. One issue mentioned was that it is sometimes hard to separate risks from other types of effects on the business. According to one interviewee, it often happens that the working group realizes that one of the risks is actually the cause of another, while others are consequences of the same. It was, therefore, requested that the model should help differentiate causes from undesirable events and consequences.

The last identified theme, *accurate scoping*, was expressed by all interviewees. They stated that it is absolutely necessary to clearly specify the object of analysis before the start of the assessment. One of the consultants described this in the following way:

> One of the most critical factors of success is to accurately scope the object of analysis. If you have bad input data, you will get nothing but bad output (Interviewee 3, 2019).

### 6.1.2 Review of the survey

To increase our chances of accurately capturing the users' needs and requirements, we sent out a survey to ten information security consultants working at Nixu in addition to conducting the interviews. The survey contained six questions, found in *Appendix B*, where the respondents were asked to grade the importance of a statement on a five-step scale ranging from *Not important* to *Very important*. As a complement to the six scale-questions, two optional free-text questions were posed.

Below is a review of the answers to each of the six scale-questions. Ten respondents constitute a small sample and general conclusions are therefore hard to draw. Instead, the responses are treated as *indicators* of factors that could be considered relevant for successful risk management models. Note that each question starts with the statement: *"How important is it to you that the risk management model…".*

1. *... is time-efficient, in terms of implementation when working with a customer?*

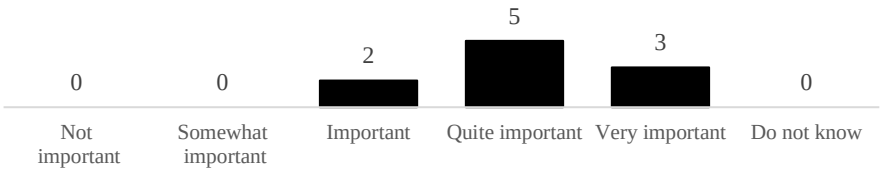



*Figure 13. Time-efficiency - costumer implementation.*

As shown in Figure 13, time-efficiency in terms of implementation when working with a customer was considered at least *Important* by all surveyed consultants. The majority of respondents selected *Quite important*, indicating that most consultants value that the implementation of the model is simple and fast when working with a customer.

2. *... is time-efficient, so that you as a consultant can understand and make use of the model in a time-efficient manner?*


*Figure 14. Time-efficiency – consultant understanding.*

To interpret the results regarding time-efficiency in terms of being easily applied and understood by the consultant (Figure 14) is not as easy as in the case of customer implementation (Figure 13). Five of the respondents chose *Somewhat important* or *Important* whereas the other half selected *Very important*. This indicates a greater spread in the opinions, but since half of the sample chose to rate time-efficiency with regards to consultant understanding as *Very important*, the factor cannot be rejected or considered irrelevant.

3. *... can handle "soft" aspects of risk (such as reputation and competitive advantage)?*

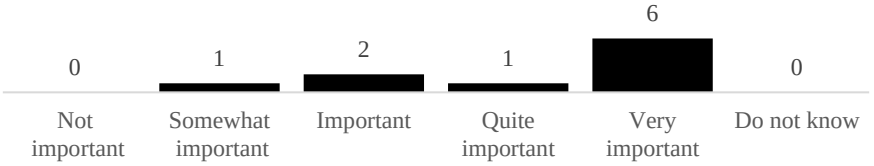



*Figure 15. "Soft" aspects of risk.*

The majority of the surveyed consultants considered it *Very important* that the risk management model can handle "soft" aspects of risk (Figure 15). Since the remaining answers vary, it is hard to draw any general conclusions other than the fact that the most common conception of softer aspects of risks within risk management is that it is very important to consider.

4. *... generates extensive results to the customer (such as detailed tables and graphs)?*

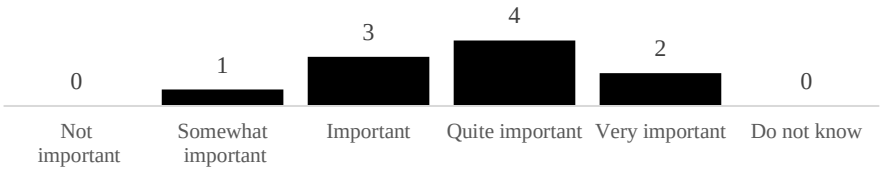



*Figure 16. Extensive results.*

The histogram's shape in Figure 16 indicates that the answers regarding extensive results to customers follow a normal distribution with mean *Quite important*. Hence, detailed information, such as tables and graphs, seems to be something the consultants' value, but do not consider crucial to the process.

5. *... generates results that are easy to communicate to management?*


*Figure 17. Communication of results – management.*

The responses regarding the importance of results being easily communicated to management leave little room for interpretation: all surveyed consultants stated that it is *Very important,* as shown in Figure 17.

6. *... generates results that are easy to communicate to the whole organization?*


*Figure 18. Communication of results – organization.*

Similar to the previous question, the consensus regarding easily communicative results to the entire organisation is clear (Figure 18). Nine out of ten respondents chose *Very important* when asked to grade how much they value that the risk management model generates results that without difficulty can be conveyed to the rest of the business.

The optional text field in the survey, where respondents could add their own suggestions of important factors in risk management, displayed a great variety of answers. The answers covered factors ranging from the importance of having a supporting tool in multiple languages to having a fact-based ground for investment decisions. The most frequently mentioned factor, however, was the importance of having a method that is easy to use as well as to reuse and update. Other mentioned factors were the need for a well-defined scope, prioritization, consistent terminology, and a better identification process.

### 6.1.3 Summary of user input

The interview and survey indicate that the users have several needs from a risk management model. All of these needs cannot be considered requirements since they are emphasized to a different degree by the users and also more or less possible to implement from our part. Below is, therefore, an outline of our transformation of these needs into *requirements*, *desires* and *unmet desires* for our model.

The first requirement identified by the authors is *communication of results.* This factor was clearly pointed out as an important factor in the survey as well as in the interviews. Communication was spoken of not only in terms of making sure that everybody uses the same terminology but also with regards to visualisation. It is therefore important that our model produces results that are easily communicated and visualized to management as well as to the organization.

The second user requirement for our risk management model, as identified by the authors, is that the model should enable *prioritization of risks*. This factor was mostly discussed during the interviews but was also suggested in the free-text area of the survey.

*Scientific grounds* is the third requirement that we have identified in the material. The consultants requested that the developed model should be more statistical than current practices and that it should be based on science, rather than subjective judgements. Our goal

is therefore to develop a model that is both logical and mathematically consistent - or simply put: built on scientific grounds.

The last identified requirements are time-efficiency and simplicity. These factors were most clearly expressed in the survey, where the importance of the model's efficiency was shown both in terms of usability when working with customers, but also when it comes to being easily understood by the consultants. We have chosen to summarize these findings using the term *practical*, which implies that the model should be easy to use in a time-efficient manner.

Apart from these four requirements the users also expressed additional desires for the model. These needs will not be a part of the requirements but are clearly relevant to the users and will, therefore, be handled to some degree in the construction of our model. One of these desires is that the model should offer *support for estimating the likelihood and impact* of potential risks. This need could, for example, imply that the model should provide suggestions on how to proceed when the analyst feels like it is hard to come up with quantitative estimates. Moreover, the users have a desire for a model that can handle *"soft" aspects of risks*, such as reputation or competitive advantage, and help the users quantify these. One last desire that was identified in the survey was that the model should provide *extensive results* to the customers, such as graphs and tables. This need was not brought up in the interviews but will be taken into account in the model since most of the survey respondents stated that this factor is quite important.

Lastly, we should mention a few unmet desires that were brought up by the consultants, but which will not be considered in the development of the risk management model. First of all, the need for *competent personnel* was expressed by all interviewees. This is, of course, an important factor of the risk management process but has been considered impractical to handle since the model cannot affect who participates in the assessment. Moreover, the need for *review*, *support in risk identification* and *scoping* is outside of the scope of this project (see Figure 4 section *4.2 Model development*) and will therefore not be handled here.

In summary, the user requirements (UR) found in Figure 19 will apply to our model.

| | | |
|---|---|---|
| *UR 1* | **Communicative** | The risk management model must generate results that are easy to communicate to management and organization |
| *UR 2* | **Practical** | The risk management model must be practical, in the sense that it is time-efficient and easy to use |
| *UR 3* | **Prioritized** | The risk management model must provide prioritization of the analysed risks |
| *UR 4* | **Scientific** | The risk management model must be scientific, in the sense that it is logical and use proper math |

*Figure 19. User requirements.*

## 6.2 Input from the literature

As previously stated, there exist hundreds of risk management models within the cybersecurity community today (Dubois *et al.*, 2010). This multifaced landscape has caused risk assessment results to vary largely in terms of accuracy, consistency, and utility to management (The Open Group, 2009). In order to navigate in this complex environment, a number of researchers have set out to identify and articulate characteristics that make up effective risk management methodologies. In this section, we will outline some of these requirements for successful risk management models, as found in the cybersecurity risk management literature and motivate which we have chosen to add to our list of requirements.

Perhaps the broadest definition of requirements for risk management models is provided by Jack Freund and Jack Jones in their book *Measuring and managing information risk: A FAIR approach*. Freund and Jones claim that risk analysis methods should be evaluated to at least three points (Freund and Jones, 2014, p.6):

1. Is it useful?
2. Is it practical?
3. Are the results defensible?

By useful, Freund and Jones mean that the model must be accurate and meaningful to decision-makers. The two authors claim that all qualitative models fail this evaluation since accuracy in qualitative terms is a matter of simple assumptions of subjective scales, such as 3.8 or medium. The meaningfulness of qualitative methods can also be questioned. What does a risk score of 3.8 mean? It might be worse than 2.5 (assuming that one is good and five is bad), but it is still very hard to compare these values to more quantitative considerations of decision-making, such as revenue or expenses (Freund and Jones, 2014, p.6).

The practical aspect of risk management models is crucial, according to Jones and Freund. They state that: “It does little to apply rocket science when all you really need to do is cross the street” (Freund and Jones, 2014, p.7). Hence, a successful risk management model should, according to Jones and Freund, be easily applicable when needed, while still enabling the assessor to go deep if necessary (Freund and Jones, 2014, p.7).

The last stated criteria by Jones and Freund is that the model should produce defensible results. According to Jones and Freund, a legitimate risk analysis model can be recognized by the presence of a rate of occurrence and a clearly stated consequence, and whether the model treats the risk problem in probabilistic terms. Once again, qualitative models often fail since they rarely explicitly state the rate of occurrence or the consequence (Freund and Jones, 2014, p.8).

Two other authors that have also studied how to evaluate risk management models are W.M Garrabrants and A.W Ellis. In their publication *CERTS: A comparative evaluation method for*

*risk management methodologies and tools* from 1990, they describe seven criteria that embody a successful risk management model. In Figure 20 these requirements are stated as in Garrabrants and Ellis' report (Garrabrants *et al.*, 1990, p. 255):

*Consistency:* Given a particular system configuration, results obtained from independent analysis will not significantly differ.

*Usability:* The effort necessary to learn, operate, prepare input, and interpret output is generally worth the results obtained.

*Adaptability:* The structure of the method or tool can be applied to a variety of computer system configurations (and the inputs can be easily updated as they periodically change).

*Feasibility:* The required data is available and can be economically gathered.

*Completeness:* Consideration of all relevant relationships and elements of risk management is given.

*Validity:* The results of the process represent the real phenomenon.

*Credibility:* The output is believable and has merit.

*Figure 20. Requirements for risk management models - Garrabrants et al., 1990.*

A more recent publication, also dedicated to the topic, is the global consortium The Open Group's *Technical guide on requirements for risk assessment methodologies* from 2009. Here, ten so-called *key risk assessment traits* are identified, each indicative of how a successful risk management methodology should perform (The Open Group, 2009, p.4-7). The Open Group's traits are summarized in Figure 21 on the next page.

*Probabilistic:* A good risk assessment methodology is based on probabilistic methods and assist the analyst in creating probabilities for risks and its component factors.

*Accurate:* A good risk assessment methodology delivers accurate results, but not necessarily precise ones. Accuracy is defined as "our capability to provide correct information", whereas precision is defined as "exact, as in performance, execution or amount".

*Consistent (repeatable):* If two analysts are given the same information independently of each other and perform a risk assessment using the same methodology, they should arrive at similar conclusions.

*Defensible:* The results of the risk assessment have to be deemed accurate and logical.

*Logical:* A good risk assessment methodology will use a model that logically describes how the world works and that does not allow for contradictory association of risk factors. Nor will a good risk assessment framework allow for mathematical expressions that are nonsensical. For example, many risk assessment frameworks that advocate the use of ordinal scales, also advocate the use of arithmetic functions on those values, and as such their results are not logical, consistent, nor defensible.

*Risk-focused:* The only metrics that really matter are the probable frequency of loss events, and the probable magnitude of loss. As a result, any assessment methodology whose end result cannot be expressed in these terms is not really measuring risk.

*Concise and meaningful:* Risk assessment results should be expressed as concisely as possible to lessen the opportunity for confusion. In order to be meaningful, recommendations from the analyst must be feasible and actionable so that the data owner can make the best decisions given the information at hand.

*Feasible:* The risk assessment model should provide feasible options to decisionmakers that are cost-effective, politically viable, and achievable from a technical and execution perspective.

*Actionable:* Risk assessment results should include a plan of action, that allows management to properly prioritize their resource allocation.

*Prioritized:* Prioritization of risks should meet the requirements of management and the results should help them to efficiently apply finite resources.

*Figure 21. Requirements for risk management models – The Open Group, 2009.*

### 6.2.1 Summary of literary input

It is hardly surprising that some of the requirements presented this section align with the requirements found during the interviews and in the survey. Hence, it is necessary to mention that some relevant requirements from the literature will not be stated as literary requirements since they have already been brought up in some form in section *6.1 Input from the users.* Three such examples are *defensible* (scientific), *prioritized* and *practical*.

It is also important to note that several of Freund and Jones' points, Garrabrants and Ellis' criteria and The Open Group's traits are actually aiming to describe the same feature, even though they are stated under different names. *Defensible* and *credibility* is one such example and *usability* and *practical* is another. Other literature-requirements, such as *risk-focused* and *feasibility*, have been considered so general and obvious that they will not be stated as requirements for our developed model. Nor will the requirements *actionable* and *completeness*, since they are outside of the scope of this thesis.

Having provided this brief motivation of literary requirements that will *not* be furthered, we are left with two requirements from the literature that will play an important role in our model. The first of these is the requirement *consistent*, meaning that the model should produce similar results no matter who performs the analysis. The second literary requirement that has been considered is *adaptable*. Here, adaptable means that the model must be applicable to a variety of organizations, much because of Nixu's broad base of customers.

In summary, the literary requirements (LR) found in Figure 22 will apply to our model.

| | | |
|---|---|---|
| *LR 2* | **Consistent** | The risk management model must be consistent meaning that it produces similar results regardless of the group or person performing the assessment |
| *LR 3* | **Adaptable** | The risk management model must be applicable to a variety of organizations and situations |

*Figure 22. Literary requirements.*

## 6.3 Additional requirements

To capture additional requirements that we consider to be missing in sections *6.1 Input from the* users and *6.2 Input from the literature*, we now turn to the last source of information: our own perceptions on risk management modelling.

From our part, it has been necessary to specify two requirements on the risk management model that we develop. First of all, we do not aim to create a model from scratch. As mentioned at several occasions throughout this thesis there are already numerous risk management models available within the cybersecurity community and our intention is to base our model on these already existing works. This means that our model will be *compound* in the sense that it will combine relevant parts from existing models, methods, frameworks and standards to make it as efficient and accurate as possible.

Moreover, our developed risk management model needs to be *balanced*. The fact that contemporary quantitative cybersecurity risk management models are often considered too complex to be implemented is described both in the literature (Wheeler, 2011, p.291) and in discussions with cybersecurity consultants at Nixu (Interviewee 3, 2019). A complex model might capture risks in a more realistic way, while a simple model might be more realistically applicable to the organization. Therefore, the risk management model must be balanced with regards to these two opposites.

In summary, the additional requirements (AR) stated in Figure 23 have been considered essential.

| | | |
|---|---|---|
| *AR 1* | **Compound** | The risk management model should be based on already existing risk management methods/models/frameworks/standards. |
| *AR 2* | **Balanced** | The risk management model must be balanced with regards to simplicity and complexity. |

*Figure 23. Additional requirements.*

# 7. Core activities

In the previous section, *6 Model requirements*, we described eight requirements that constitute the basis of our model. In this section, we proceed by turning the spotlight to the content of our model. To build an accurate cybersecurity risk management model, we have carefully studied the contemporary scientific discussion on the topic. While researching, we kept the established requirements in mind to build a model framework that suits the users' and literary needs.

As stated in section *4.2 Model development* and Figure 4, we have chosen to focus on three of the eight activities stated in the ISO 27005 risk management framework. Therefore, the activities risk analysis, risk evaluation, and risk communication have continuously been referred to as *core activities* throughout our thesis. Here, we will provide important features of each of the core activities, as found in the contemporary cybersecurity risk management literature. These features have been considered necessary and relevant based on the collected model requirements.

## 7.1 Risk analysis

Risk analysis is the third step in the risk management process according to the ISO-definition, following context establishment and risk identification. The goal of this phase is to establish a risk level for each of the identified risks so that they can be compared and evaluated. In a quantitative world, this means associating the impact of the risk with a monetary value and the likelihood with a probability. As stated in section *2.1 What is cybersecurity risk management?* the risk level is often quantitatively calculated as expected loss. In this section, each of these two sub-activities: estimation and calculation, will be outlined in detail. We will start, however, with a brief discussion on analytical maturity.

### 7.1.1 Analytical maturity

There is no simple "one-size fits all" solution to the risk management problem. Every organization is different and has its own needs when it comes to risk assessment. Some organizations have already begun using big data-methodologies such as predictive analytics, machine learning, and data science to evaluate risks, whereas others have barely started their risk management processes (Hubbard and Seiersen, 2016, p.200).

Therefore, a good place to begin your risk analysis is to recognise where your organization is on an analytical maturity scale. By understanding the organisation's prospects when it comes to risk management, it is possible to improve the odds of being cost-effective and successful in the management of risks (Freund and Jones, 2014, p.336). Freund and Jones suggest that organizations can be evaluated to a five-levelled maturity continuum (Freund and Jones, 2014, p.337). Each of the maturity levels are defined by conditions of the elements in Table 2.

*Table 2. Elements of analytical maturity (Freund and Jones, 2014, p.338-340)*

| Element of maturity | Example of questions asked |
|---|---|
| Terminology | Is there an established risk-nomenclature defined within the organization? |
| Risk concepts | Does the organization understand risk-related concept such as accuracy versus precision and subjectivity versus objectivity? |
| Visibility | Is the risk landscape visible to the organization? |
| Analysis | Which type of analysis is performed on risk issues today? |
| Decision authority | Are decision-making roles, responsibilities and limitations clearly defined? |
| Risk appetite definition | Does the organization know how much risk it is willing to handle? |
| Policies | Are the organization's defined information security policies aligned with executive management? |

There are numerous analytics maturity models available (see for example Petrie, Potter and Ankorion, 2018 and Puget, 2014) and most important is perhaps not *which* model that is used, but that the maturity of the organization *is* gauged before starting the analysis.

### 7.1.2 Estimation of risk impact and likelihood

What is needed to estimate the impact and likelihood of risks that an organization face? We would like to describe these factors using the interrogatives *who*, *what* and *how*. To answer the question of who: a working group is needed that has already identified risks that the organization face and has the right set of skills to estimate the monetary impact and percental likelihood of these risks. Usually, there is one or several experts among the group members who are particularly knowledgeable about organizational processes and economic circumstances (Hubbard and Seiersen, 2016, p.67).

Now to the question of what. In the example of a quantitative risk analysis presented in section *2.4 What are the gains of quantitative risk analysis?* the likelihood and impact were assessed as point estimates. The likelihood of Risk A was for example estimated to 2 % whereas the impact was estimated to 400 000 SEK. In a real-life scenario, however, it is often hard to reach such precise conclusions. Uncertainty is most of the time inevitable, and it is, therefore, preferable to assess the likelihood and impact in less definite terms. One solution to this problem is to estimate the impact and likelihood as *ranges*. By doing so, the assessor is no longer forced to come up with unrealistically precise values but is given the possibility to express his or her uncertainty about the estimate (Hubbard and Seiersen, 2016, p.135).

Now that we know who is estimating (the working group) and what to estimate (impact and likelihood in terms of ranges), we also need to know how to do it. There are many ways in which the impact and likelihood of risks can be assessed. The most preferable source of information is, of course, objective historical data. Nonetheless, it is often the case that this type of data is not available and this is where the expert component comes to play (Hubbard and Seiersen, 2016, p.76).

#### 7.1.2.1 Improving expert estimations

Expert-based risk-estimation is the most common way to carry out risk assessments within the cybersecurity community today (Hubbard and Seiersen, 2016, p.64). Letting an expert provide estimates of the likelihood and monetary impact of risks is often the most available and efficient form of assessment. But it should be treated with caution. As Hubbard and Seiersen argue in their book, several studies have pointed to the fact that experts are often highly inconsistent in their estimations and that even trained scientists tend to greatly misestimate the odds when new data is used to confirm or contradict previous estimates (Hubbard and Seiersen, 2016, p.70).

To improve this human component of quantitative risk estimation, a number of authors have suggested different practices to advance experts' forecasting abilities. Hubbard and Seiersen refer to this betterment of subjective estimates by using the term *calibration* (Hubbard and Seiersen, 2016, p.154). They prove that training has a significant effect on how experts make estimations and claim that every risk management expert must, therefore, understand his or her own biases and learn how to handle uncertainty – in Hubbard and Seiersen's words: they must be calibrated (Hubbard and Seiersen, 2016, p.136). In Figure 24 on the next page, we will briefly outline nine such *calibration techniques* that can help experts provide more accurate quantitative estimations. For those who are interested, a more thorough explanation for some of the techniques is provided in *Appendix D*.

#### 7.1.2.2 Decomposing risks

Even highly calibrated experts can still have troubles estimating the likelihood and impact of risks. Therefore, it is relevant to highlight other techniques that can be used for improving estimations. One suggestion commonly brought up by authors within the field of quantitative risk management is to decompose risks (Hubbard and Seiersen, 2016, p.75).

Decomposing basically means to think about risks in smaller segments, that are more tangible and easier to envisage. This key technique is sometimes referred to as *disaggregation*. Let us say for example that you are to estimate the monetary value of a denial of service (DOS) attack on a given system. Instead of trying to estimate the total impact directly, you could break down the impact into components that are easier to estimate. A few such examples are the duration of the attack, the number of people affected and the cost per person affected. A well-performed disaggregation often results in more accurate estimates (Vose, 2008, p. 401).

***Anti-anchoring:*** Be aware of the anchoring-effect, meaning that you should notice that your estimates can be affected by numbers you had in your head before the assessment (Tetlock, 2015, p.120).

***BOESAT:*** Let a "Bunch Of Experts Sit Around Talking". Talking about issues together can reduce errors that individual estimates manifest, but be careful so that groupthink does not emerge (Clemen and Winkler, 1999).

***Bracketing:*** Use an absurdity test to estimate the likelihood and impact. Start with extremely wide ranges and narrow them down by eliminating highly unlikely values (Hubbard and Seiersen, 2016, p.145).

***Combine expert estimates:*** Let several experts make individual estimations and combine these using mathematical operations. A common, well-functioning method is to simply average the expert estimates (Clemen and Winkler, 1999).

***Consider two pros and two cons:*** Think of at least two reasons why your estimates could be wrong, as well as two reasons why you should be confident in them (Hubbard and Seiersen, 2016, p.145).

***Consistency checking:*** Test if the expert is making different estimates when asking the question differently or at a different time. You can also try if the expert is making similar estimates as other experts: are they in consensus? (Hubbard and Seiersen, 2016, p.72)

***Equivalent bet test:*** Set up an equivalent bet test for each estimate that the expert come up with. Increase the stakes by asking the expert if that person is willing to bet 10 000 SEK of his or her own money on the forecast (Hubbard and Seiersen, 2016, p.141).

***Red teaming:*** Find alternative arguments to the prevailing view and seek out information that do not support the current theory. The red team acts as "the devil's advocate" (Mulvaney, 2012).

***Repetition and feedback:*** Make sure that the expert is provided feedback on his or her performance. This can be done by making several assessments in succession, evaluating how well the expert performed and trying to improve the estimates to the next round (Hubbard and Seiersen, 2016, p.145).

*Figure 24. Calibration techniques for improved expert estimations.*

Another decomposition strategy, suggested by Hubbard and Seiersen, is to decompose the impact according to the CIA-triad. The CIA-triad is a commonly used model within cybersecurity that aims to guide organizations on how to develop security policies with regards to three fundamental aspects of information-systems: Confidentiality, Integrity, and Availability. Briefly, these three cornerstones of cybersecurity relate to the improper disclosure of information (confidentiality), modification of data (integrity) and the availability of data when it is needed (Pfleeger, Pfleeger, and Margulies, 2015). Hubbard and Seiersen argue that some companies find it easier to decompose risks according to the CIA-triad since many are already familiar with the model (Hubbard and Seiersen, 2016, p.114).

An additional example of a decomposition strategy for impact is provided by Freund and Jones in their FAIR model. They propose that risks can be segmented into six forms of losses: productivity, response, replacement, competitive advantage, fines, and judgements and reputation. According to Freund and Jones, productivity and replacement costs mostly occur as primary losses whereas the three latter tend to appear as secondary losses. Response losses are costs associated with managing loss events and these commonly occur both as primary and secondary losses (Freund and Jones, 2014, p.66). The six forms of losses are summarized in Table 3.

*Table 3. Jones and Freunds' six forms of losses*

| **Typical primary losses** | **Typical secondary losses** |
|---|---|
| Productivity | Competitive advantage |
| Replacement | Fines and judgements |
| Response | Reputation |

Is decomposition always favourable? No, not in cases where the problem is “over-decomposed” so that the segments actually introduce more uncertainty than your simpler model initially had. An informative decomposition is one where the cybersecurity expert can utilize the knowledge that he or she has about the environment so that the decomposed risks are less abstract to the expert than the aggregated amount. If not, it is probably better to stay with the original state (Hubbard and Seiersen, 2016, p.76, 121).

#### 7.1.2.3 The importance of documentation

We have now described how to improve estimates by calibrating experts and decomposing risks into smaller segments, but there is one more crucial component to the estimation of impact and likelihood. In order not to repeat the same mistakes over and over in your risk management process, it is absolutely necessary to *document* the scope of analysis and the reasoning and basis for each estimated value. Having stated the rationale behind each number

enables later reviewing and reuse of the analysis since it will help you understand where a specific number came from (Freund and Jones, 2014, p.100-101).

### 7.1.3 Computation of risk level

The most central activity in the risk analysis occurs after the estimation of likelihood and impact, namely the measurement of the risk. The name of the result of this activity varies in the literature, some referring to it as a measure of *risk level* (ISO 27005, 2018) and others as *risk exposure* (Wheeler, 2011, p.38). As stated in section *2.1 What is cybersecurity risk management?* we have chosen to use the term risk level.

A well-known quantitative measure of risk level is expected loss, calculated by multiplying the likelihood and the impact as shown in Equation 7 (Wolke, 2017, p.12).

$$Expected\ Loss = Impact \cdot Likelihood \tag{7}$$

When calculating the quantitative risk level, it is necessary to state a timeframe. Are you estimating risks that can occur a year from now? A month? As described in section *2.1 What is cybersecurity risk management?* we have chosen to use expected loss as quantitative measure of risk level in this thesis. It is fair to mention, however, that there is also another frequently used term for describing the quantitative risk level, namely Annualized Loss Expectancy (ALE). The ALE, found in Equation 8, is simply the expected loss with a preset timeframe of one year. The first factor in the equation, Single Loss Expectancy (SLE), is what we have chosen to call impact: a monetary measure of the loss related to risk. Similarly, we measure the second factor, Average Rate of Occurrence, in terms of likelihood (Wheeler, 2011, p. 40).

$$Annualized\ Loss\ Expectancy = Single\ Loss\ Expectancy \cdot Average\ Rate\ of\ Occurace \tag{8}$$

The equations of expected loss and ALE indicates that precise values are used for impact and likelihood. This raises the question of how the range estimates come to play in the calculations? The short answer is that the range estimations are used to model the experts' uncertainty as distributions. Depending on which distribution we use for modelling, the calculations to obtain the distribution varies, as described in section *5 Statistical aspects of risk management modelling*. When the distributions – based on the range estimations – are computed, we make simulations with numbers drawn from these distributions. This means that the values for impact and likelihood in Equation 7 will be regenerated for each simulation, resulting in new calculations of expected loss for each run.

## 7.2 Risk evaluation

The last step of the risk assessment process is risk evaluation. During the risk evaluation phase, the assessor produces a list of prioritized risks and decides on which future actions should be taken based on the provided risk picture (ISO 27005, 2018). From the preceding

step, risk analysis, all risks have been given a risk level measured as expected loss. One way of evaluating the risks is thus to simply sort the risks based on the expected loss (Vose, 2008, p. 159).

This simplicity is one of the obvious advantages of using expected loss as a measure. It provides a straightforward way of making comparisons between risks as well as providing clear indications of which risks to prioritize (Freund and Jones, 2014, p.107-109). It is important to remember, however, that expected loss only offers one perspective. Suppose, for example, that a risk has an extremely small likelihood but a catastrophic potential impact. When multiplying these values, the resulting expected loss might not be noteworthy due to the fact that the minimal likelihood will degrade the product. The consequences of such an event could be catastrophic for an organization - something the comparisons of expected loss will not reveal. Thus, another perspective worth analysing is the size of the impact itself. This highlights the fact that the evaluation should not only focus on one single measure, but rather help management to make well-informed decisions by providing multiple alternative perspectives (Freund and Jones, 2014, p.107-109).

In order to model expert estimations, several professionals within the risk management field argue for using distributions as input to the analysis (Vose, 2008; Freund and Jones, 2014; Hubbard and Seiersen, 2016). To give the analysis even more credibility, the output can be modelled as distributions as well by making use of simulations. By presenting the results as distributions we enable evaluation of the uncertainty and variability of our results. For example, we can present the statistical measures minimum, mean, most likely, and maximum value of the impact distribution for each risk, which gives a more detailed and accurate description of possible outcomes (Freund and Jones, 2014, p.107-110).

We can add dimensions to the evaluation by dividing the impact of each risk in parts of interest. For example, an organisation could be interested in comparing risks' impacts divided in the previously described six forms of losses (see Table 3). This would require the working group to estimate the impact of each form of loss and risk. Based on the divided impact estimations, the expected loss can be simulated and presented for each loss form. Such evaluation could be valuable when one loss form, for example reputation, is especially important to an organisation. To make the results even more informative, the statistical measures of the expected loss distribution (min, mean, most likely, and max) can be presented for each loss form, as described in section *5.3 Statistical measures.*

Dividing the impact into parts of interest is one way to add information to the evaluation. However, it is also important to keep in mind that all additional dimensions both require more work from the assessors as well as more time from those trying to understand the results (Freund and Jones, 2014. p.107-120). As is stated by Wheeler, it is often better to start small, making small-scale assessments, and increase the complexity as the organization reaches a higher degree of analytical maturity when it comes to risk management. Otherwise, there is a great risk that your organization will continuously be wasting time and resources struggling with fundamental process issues (Wheeler, 2011, p.289).

## 7.3 Communication of results

How information is presented to decision-makers should be adjusted depending on the purpose of the risk assessment, but also on the organisation's preferences. The global IT-consortium The Open Group suggests that the six questions *who, what, when, where, why* and *how* should be used when deciding how to communicate results to decision makers (The Open Group, 2018).

Here, we will focus on the two interrogatives how and what, starting with a discussion on how risks should be communicated. A model's results can be presented in numerous ways, often using either single values or graphs. Whereas numbers are more informative by providing raw data and statistics, graphs have the advantage of presenting the information in a more intuitive way. Thus, graphical presentations are often preferred when communicating a model's results (Vose, 2008, p.71).

One of the most commonly used graphs in risk analysis is histograms, which are generated by grouping the data in different bars or classes. The number of values within each class is divided with the total number of values to compute their respective densities. The histogram plot is a good way of illustrating the distribution of a variable but cannot be used to read off a certain probability associated with an x-axis value. To determine quantitative information from a plot, one can instead use a descending cumulative frequency plot, which shows the probability of being greater than the x-axis value. Cumulative frequency plots are often used when modelling costs (Vose, 2008, p.70-76). A third way of graphically presenting results from the risk analysis is to use scatterplots. The axes in the scatterplot can be used to represent the likelihood and the impact, and each dot to represent one risk simulation placed in the plot based on its simulated likelihood and impact value (Freund and Jones, 2014, p.110-111).

Freund and Jones build on the discussion of how to communicate results by recognizing that previous work has not clearly distinguished the difference between how a risk analysis is carried out and how the results are presented. They argue that a quantitative analysis can be presented qualitatively. An advantage of such translation is that qualitative presentation of results are good at giving clear indications of which risks are most critical to handle. Management responsible for making decisions often have limited time and therefore appreciate clear indicators of when things are amiss, such as the red colour describing the most critical risks in the risk matrix. Freund and Jones, therefore, propose that a heat map can be used to translate quantitative analysis to qualitative results (note that the reverse translation does not apply). The advantage of such a visualisation is that the simple, qualitative indication of the severity of risks is available, while it is still possible complement the communication with more informative, quantitative visualisations (Freund and Jones, 2014, p.106-107).

The second interrogative we focus on – the what – relates to what to include in the communication of results. Freund and Jones emphasize the importance of presenting the output distribution when using an input distribution. Communicating the output distribution

generated by simulations, instead of a single value, increases the credibility of the analysis since it conveys the uncertainty of the assessment. The output distribution can be presented in several ways, such as a table containing the maximum, mean and minimum value of simulations, a histogram, or a scatterplot (Freund and Jones, 2014, p.106-110).

Relating to the discussion of what to communicate, are the suggestions proposed by the experienced risk analyst David Vose (2008). He states that one of the most important things to consider concerning risk communication is to keep the results simple. Vose argues that it is probably better only to communicate a few statistical measures that are easy for decision-makers to understand than to provide too much complex information. He suggests that cumulative percentiles, such as the probability of being above or below a certain amount, together with the mean and a measure of spread usually communicate all the information decision-makers need (Vose, 2008, p.91-92).

# 8. The MaRiQ Model

We have now reached the last section of the third part of this thesis. Having provided the requirements that constitute the base of our model as well as the core activities that comprise its content, it is time to describe our risk management model in its entirety. We have chosen to name our model MaRiQ since its purpose is to Manage Risks Quantitatively. We will start off by providing a flowchart of the model along with a model description, followed by an explanation of the tool that supports MaRiQ and its statistical considerations. Lastly, we will outline how the model was perceived in a real-life client-case.

## 8.1 Description of the MaRiQ Model

A high-level view of the MaRiQ model is specified in Figure 25Figure 3. As is shown, the process consists of three main activities, each of which provides a number of steps to follow. In total, the process entails eleven steps that need to be performed in sequential order. In the description of these steps on the following pages, the symbol of two hammers (⚒) means that the accompanying MaRiQ tool supports the specified procedure. How the tool aids in the different steps will be furthered outlined in section *8.2 Description of the MaRiQ* Tool.

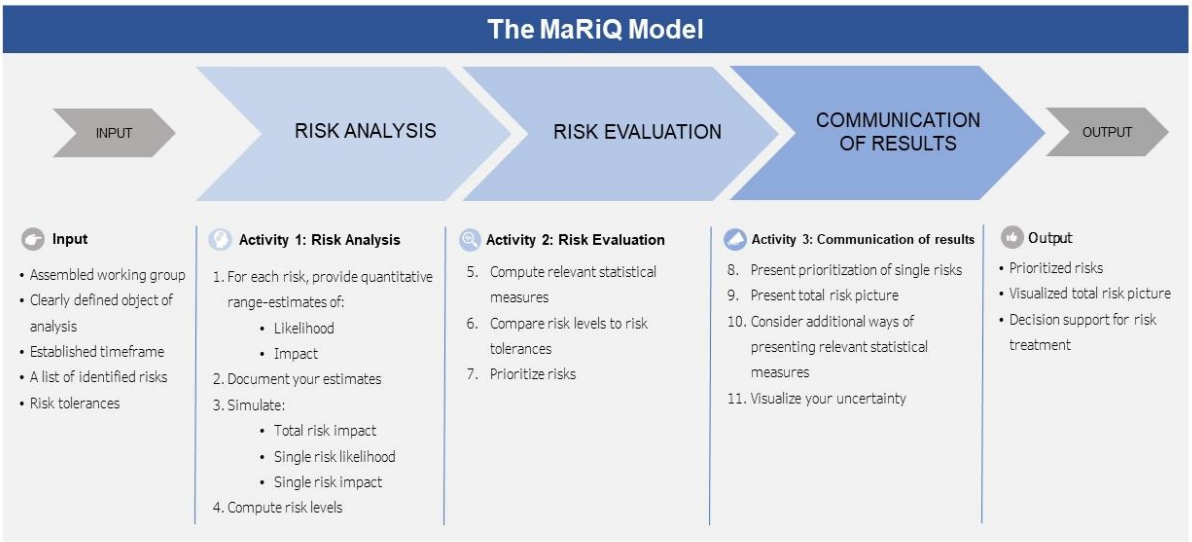



*Figure 25. Process model of MaRiQ.*

Before getting into the details of the activities and steps, it is fair to remind the reader that MaRiQ is intended to hook on to the already existing ISO 27005 risk management framework. Therefore, the model needs a well-reasoned input to function. As shown in Figure 25, this input consists of an already assembled working group, a clearly defined scope and object of analysis, an established timeframe, a list of identified and validated risks that the organization face, and estimations of the organization's risk tolerances.

After having completed the MaRiQ process, an output will be produced that consists of risks prioritized according to the organization's objectives, an overview of the total risk picture as well as information that constitute a solid decision basis for the proceeding ISO 27005 activities risk treatment and risk acceptance.

### 8.1.1 Activity 1: Risk analysis

**Input:** An assembled working group, a defined object of analysis, an established timeframe, a list of identified risks, and risk tolerances

**Goal:** To estimate the impact and likelihood and calculate the risk level

**Output:** Total and single risk simulations and risk level calculations

#### *Step 1. For each risk, provide quantitative range-estimates of likelihood and impact*

For each of the risks provided as input to MaRiQ, the working group should provide range-estimates of the impact and the likelihood. Each of the two factors should be estimated using a confidence interval, which means that the confidence level corresponds to the chance of the range containing the right answer. The purpose of the confidence interval is to capture the uncertainty of the assessor as well as the variability of the impact and likelihood.

Likelihoods should be assessed by providing a confidence interval as a percentage-range, representing the likelihood that the risk will occur. As an example, an expert might say: "Within our stated timeframe, I am 90 % certain that Risk A will occur with a likelihood between 5% and 10%". If the stated timeframe is, for example, one year, this would imply that the risk occurs between five and ten times every hundred years.

Impacts should be assessed by providing a confidence interval of the potential monetary loss if that risk was to occur. An expert might for example reach the following conclusion: "I am 90 % certain that if Risk A occurred, the monetary impact would be between 40 000 and 50 000 SEK".

If you are struggling to find reasonable estimates for the impact and likelihood, we suggest using calibration techniques or decomposition strategies, as stated in Table 4. If none of them suit your organization, feel free to come up with your own decomposition strategies or techniques for improving expert estimates.

*Table 4. Techniques and strategies for improving estimations of likelihood and impact*

| Calibration techniques | Decomposition strategies |
|---|---|
| Anti-anchoring | Disaggregation |
| BOESAT | CIA-triad |
| Bracketing | Six forms of losses |
| Combine expert estimates | |
| Consider 2 pros and 2 cons | |
| Consistency checking | |
| Equivalent bet test | |
| Red teaming | |
| Repetition and feedback | |

#### *Step 2. Document your estimates* ⚒

In order to make the assessment revisable, it is absolutely necessary to document the reasoning behind the working group's estimates. Documentation can be done in any way suitable for the organization, but we suggest that you document your results so that they are easily accessible for those who will review, update and reuse the assessment.

#### *Step 3. Simulate total and single risks* ⚒

Using a software, potential outcomes of the total and single risk scenario should be simulated. Preferably, the statistical technique Monte Carlo is used with a *large* number of simulations.

The total risk impact is simulated by letting the software evaluate whether each risk occurs or not. If the risk is simulated as occurring, the software proceeds by finding the risk impact. When all risks have been simulated once, the impact for that scenario is calculated by summarizing the impacts of the risks that did happen.

The single risk impact and likelihood is computed by randomly simulating a number from their respective distributions.

#### *Step 4. Calculate risk levels* ⚒

Using a software, the risk level for each of the identified risks should be calculated. The risk level is expressed as expected loss and is calculated as the product of each simulated likelihood and impact, for each risk.

### 8.1.2 Activity 2: Risk evaluation

**Input:** Total and single risk simulations and risk level calculations

**Goal:** To compare the risks and evaluate them against your risk tolerance

**Output:** Prioritized risks and relevant statistical measures

#### *Step 5. Compute relevant statistical measures* ⚒

Provided the simulated values and computed expected loss from the risk analysis, use a software to compute relevant statistical measures from the data. Which these statistical measures are depend on your organization, but some of the most common ones are measures of location, measures of spread and measures of shape.

#### *Step 6. Compare risk levels to risk tolerances* ⚒

Manually or digitally, the risk levels should be compared to the risk tolerances that were provided as input to the assessment. Is the total risk impact exceeding the organization's total impact tolerance? Do some single risks seem to come with a higher impact than what the organization can withstand?

#### *Step 7. Prioritize risks* ⚒

Manually or digitally, the working group must compare their single risks against each other. Which ones seem to come with the highest expected loss? Does some risk introduce an extreme potential impact? Are some risks so likely to occur that they simply cannot be disregarded? No matter how the working group chooses to prioritize their risks, it must be done based on the organization's objectives and the target group of the assessment.

### 8.1.3 Activity 3: Communication of results

**Input:** Prioritized risks and relevant statistical measures

**Goal:** To visualize the result of the assessment so that relevant stake-holders understand the risk situation

**Output:** Different presentation forms

#### *Step 8. Present prioritization of single risks* ⚒

Single risk prioritization should be visualized in a way that enables relevant stakeholders to perceive the information in a time-efficient manner. A list or a table of risks with accompanying expected loss, impact and/or likelihood is one suggestion. The single most

important thing to consider is that the visualization suits the decision makers and provides information that enables grounded decisions.

#### *Step 9. Present total risk picture* ⚒

To present the simulations of the total risk picture, we suggest creating a graph with two curves: one showing the total risk tolerance and one the total risk impact. Having these two in the same chart, it is possible to overlook your total risk picture. Does your organization seem to have less total risk impact than tolerated? Or is the total risk impact exceeding the risk tolerance?

#### *Step 10. Consider additional ways of presenting relevant statistical measures* ⚒

There are many ways in which risks can be communicated. Graphs, colours, tables, and patterns are all examples of features the working group can use to highlight or present risks in different ways. The working group should carefully consider how the recipient or recipients of the assessment will most efficiently absorb the information and adapt their visualizations thereafter.

#### *Step 11. Visualize your uncertainty* ⚒

There are many ways in which the uncertainty of the working group's assessments can be presented. A table sorted on the size of the range-estimate of each risk, a scatterplot showing all simulated outcomes of likelihood and impact or a matrix containing the minimum, mean and maximum value of each risk are just a few such examples. Which type of visualization that is used is less important than the fact that the uncertainty *is* visualized. By clearly presenting the spread of the simulated results, decision makers are reminded of the embedded uncertainty as well as natural variations of future outcomes.

## 8.2 Description of the MaRiQ Tool

To facilitate the implementation of our risk management model, we constructed a tool in Excel that supports relevant parts of the MaRiQ model. The functionality of the tool was developed using Visual Basic for Application (VBA) scripts, whereas the majority of the interface was designed using predefined Excel functions and features.

In this section we will present two relevant aspects of the tool: First, we will describe what the MaRiQ tool looks like and outline each of its subprocesses in detail. Second, we will motivate the statistical considerations that we have made, constituting the basis of the tool's functionality.

### 8.2.1 Tool overview

The MaRiQ tool consists of the following five worksheets:

- About
- Estimations
- Documentation
- Results – Single Risks
- Results – Total Risks

As the name suggests, the About-worksheet provides an overview of the tool and information on how to get started. A print screen of the worksheet is provided in Figure 26 below.

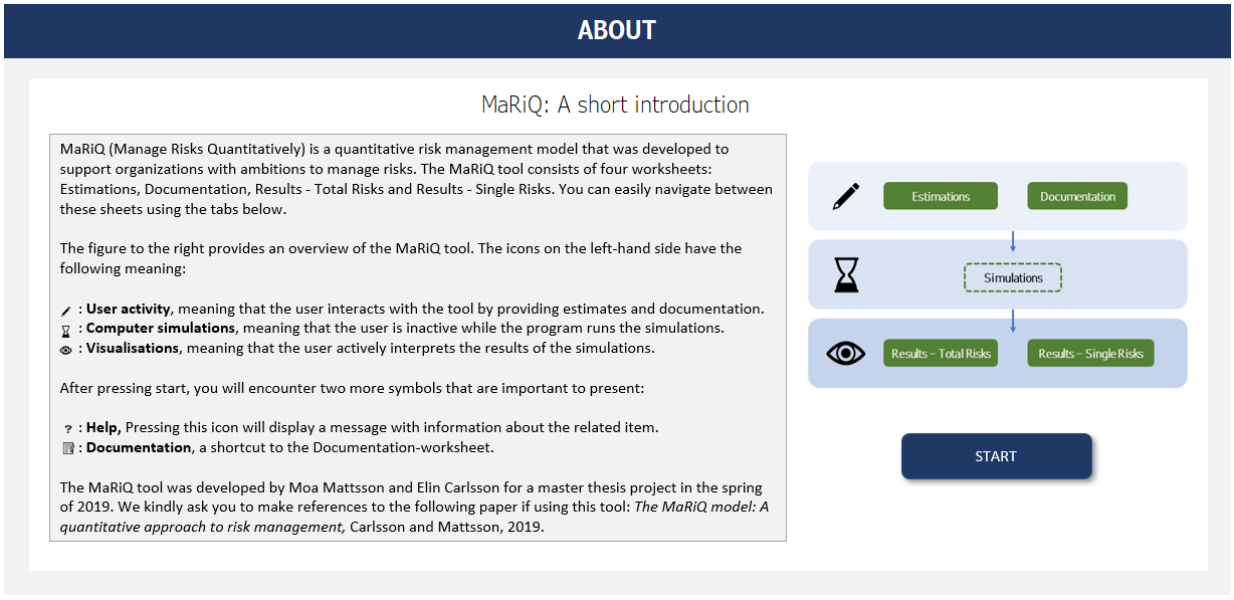



*Figure 26. The About-worksheet.*

To the left in Figure 26, there is a grey square containing information on how to use the MaRiQ tool. To the right, there is an image describing where in the process the user will encounter the four remaining worksheets (Estimations, Documentation, Results – Total Risks and Results – Single Risks). As one can see, these worksheets appear in three different blocks. In the first block, represented by the icon of a pen, the user interacts with the tool by providing estimates of the risks and by documenting the reasoning behind these estimates. In the second block, represented by a time glass-icon, the user is inactive while the program runs the simulations. The third block is represented by the icon of an eye, and this is where results are visualized for interpretation by the assessor.

By pressing the *Start button*, the user is forwarded to the Estimations-worksheet where he or she can initialize the simulation process.

### 8.2.1.1 Estimations

The Estimations-worksheet is where the user enters his or her estimates of the identified risks. As shown in the columns of the leftmost table in Figure 27, there are three estimation-inputs required from the user: the name of the risk, the estimated likelihood range, and the estimated impact range. It is possible to enter up to 50 risks in the worksheet.

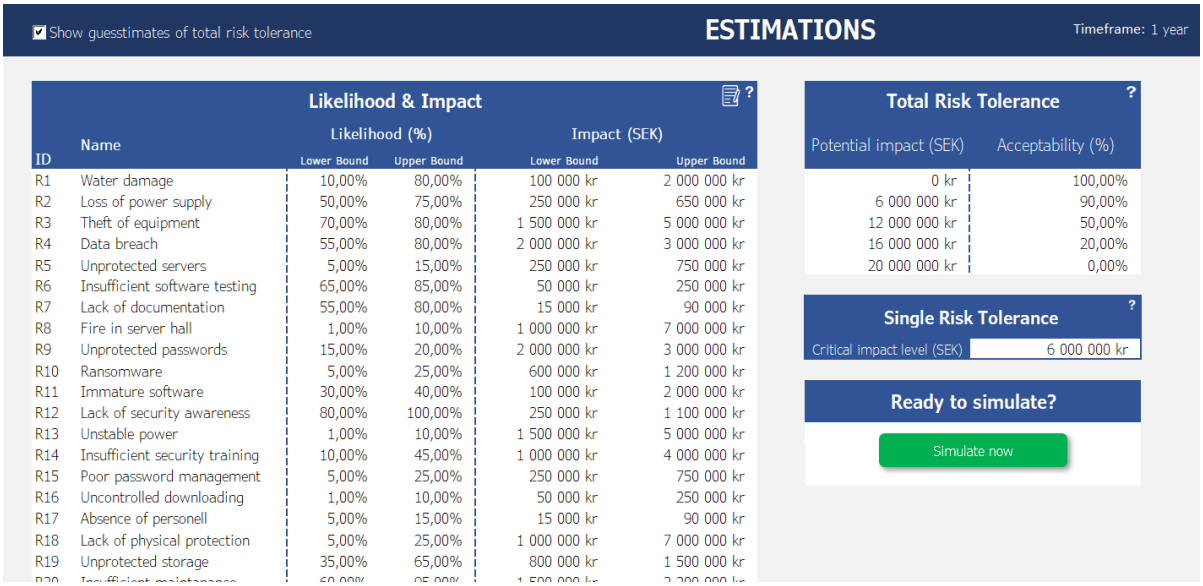


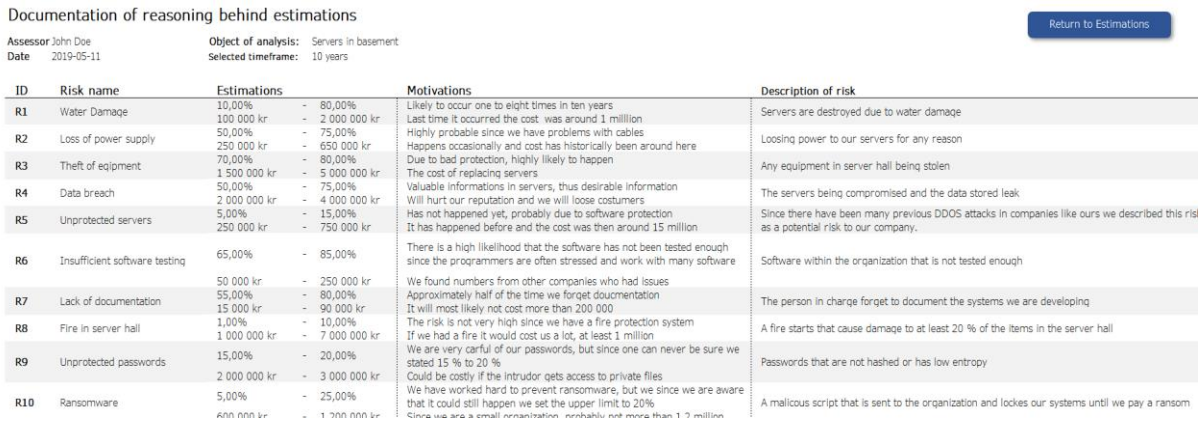

*Figure 27. The Estimations-worksheet.*

In addition to the impact and likelihood estimations, the user is encouraged to provide the total risk tolerance of the organization, which is entered in the top-right table in Figure 27. The purpose of the total risk tolerance is to achieve an acceptability reference to which the total risk picture can be compared. The most important value for the user to enter is the 0% acceptability, which should equal the total monetary loss that the organization cannot accept under any circumstances. In Figure 27, the 0% acceptability is for example set to 20 million SEK, which means that the organization cannot accept a chance of losing 20 million SEK or more. In the same way, the gradient scale leading up to the 100% acceptability, answers the question: can we accept an *x* % probability of losing *y* SEK or more? As is shown in the top-left corner of Figure 27, the MaRiQ tool offers the possibility to provide guesstimates of the total risk tolerance by clicking a checkbox. These guesses are made through a primitive algorithm, based on the 0% acceptability level stated by the user.

Moreover, the user is encouraged to provide a single risk tolerance. The single risk tolerance is an estimate of how much loss an organization can handle, caused by a single loss event. As opposed to the total risk tolerance, this measure aims to capture risks that can single handedly cause great damage to the organization if they occur. Let us say, for example, that we know that a loss of more than 2.5 million SEK could result in the liquidation of the organization, thus our single impact tolerance should be set to 2.5 million SEK.

Having provided range-estimates for each risk, the total risk tolerance and the single risk tolerance, the user is almost ready to start simulating. This is done by pressing the green button reading *Simulate now*. Before doing so, however, we recommend the user to document the reasoning behind each estimate. This can be done in any way suitable for the organization, but the MaRiQ tool lets the user file motivations in a worksheet called Documentations. The Documentations-worksheet is reached by pressing the logo of a paper and pen in the header of the *Likelihood & Impact* table, as shown in Figure 27.

### 8.2.1.2 Documentation


Documentation of reasoning behind estimations

Return to Estimations

Assessor John Doe
Date 2019-05-11

Object of analysis: Servers in basement
Selected timeframe: 10 years

| ID | Risk name | Estimations | | | Motivations | Description of risk |
|---|---|---|---|---|---|---|
| R1 | Water Damage | 10,00%<br>100 000 kr | -<br>- | 80,00%<br>2 000 000 kr | Likely to occur one to eight times in ten years<br>Last time it occurred the cost was around 1 milllion | Servers are destroyed due to water damage |
| R2 | Loss of power supply | 50,00%<br>250 000 kr | -<br>- | 75,00%<br>650 000 kr | Highly probable since we have problems with cables<br>Happens occasionally and cost has historically been around here | Loosing power to our servers for any reason |
| R3 | Theft of eqipment | 70,00%<br>1 500 000 kr | -<br>- | 80,00%<br>5 000 000 kr | Due to bad protection, highly likely to happen<br>The cost of replacing servers | Any equipment in server hall being stolen |
| R4 | Data breach | 50,00%<br>2 000 000 kr | -<br>- | 75,00%<br>4 000 000 kr | Valuable informations in servers, thus desirable information<br>Will hurt our reputation and we will loose costumers | The servers being compromised and the data stored leak |
| R5 | Unprotected servers | 5,00%<br>250 000 kr | -<br>- | 15,00%<br>750 000 kr | Has not happened yet, probably due to software protection<br>It has happened before and the cost was then around 15 million | Since there have been many previous DDOS attacks in companies like ours we described this ris as a potential risk to our company. |
| R6 | Insufficient software testing | 65,00%<br><br>50 000 kr | -<br><br>- | 85,00%<br><br>250 000 kr | There is a high likelihood that the software has not been tested enough since the programmers are often stressed and work with many software<br><br>We found numbers from other companies who had issues | Software within the organization that is not tested enough |
| R7 | Lack of documentation | 55,00%<br>15 000 kr | -<br>- | 80,00%<br>90 000 kr | Approximately half of the time we forget doucmentation<br>It will most likely not cost more than 200 000 | The person in charge forget to document the systems we are developing |
| R8 | Fire in server hall | 1,00%<br>1 000 000 kr | -<br>- | 10,00%<br>7 000 000 kr | The risk is not very high since we have a fire protection system<br>If we had a fire it would cost us a lot, at least 1 million | A fire starts that cause damage to at least 20 % of the items in the server hall |
| R9 | Unprotected passwords | 15,00%<br>2 000 000 kr | -<br>- | 20,00%<br>3 000 000 kr | We are very carful of our passwords, but since one can never be sure we stated 15 % to 20 %<br>Could be costly if the intrudor gets access to private files | Passwords that are not hashed or has low entropy |
| R10 | Ransomware | 5,00%<br>600 000 kr | -<br>- | 25,00%<br>1 200 000 kr | We have worked hard to prevent ransomware, but we since we are aware that it could still happen we set the upper limit to 20%<br>Since we are a small organization, probably not more than 1 2 million | A malicous script that is sent to the organization and lockes our systems until we pay a ransom |

*Figure 28. The Documentation-worksheet.*

The risk names and estimates that the user entered in the Estimations-worksheet are automatically transferred to the Documentation-worksheet, as is shown in Figure 28. In the Documentation-worksheet, the user is asked to provide the name of the object of analysis and of the assessor. The user is also encouraged to state the motivations behind each of the estimated likelihoods and impacts and, if possible, describe each of the identified risks. The purpose of the Documentation-worksheet is to enable review and reuse of the analysis and to allow for subsequent assessors to understand how their predecessors reasoned.

### 8.2.1.3 Results – Single Risks

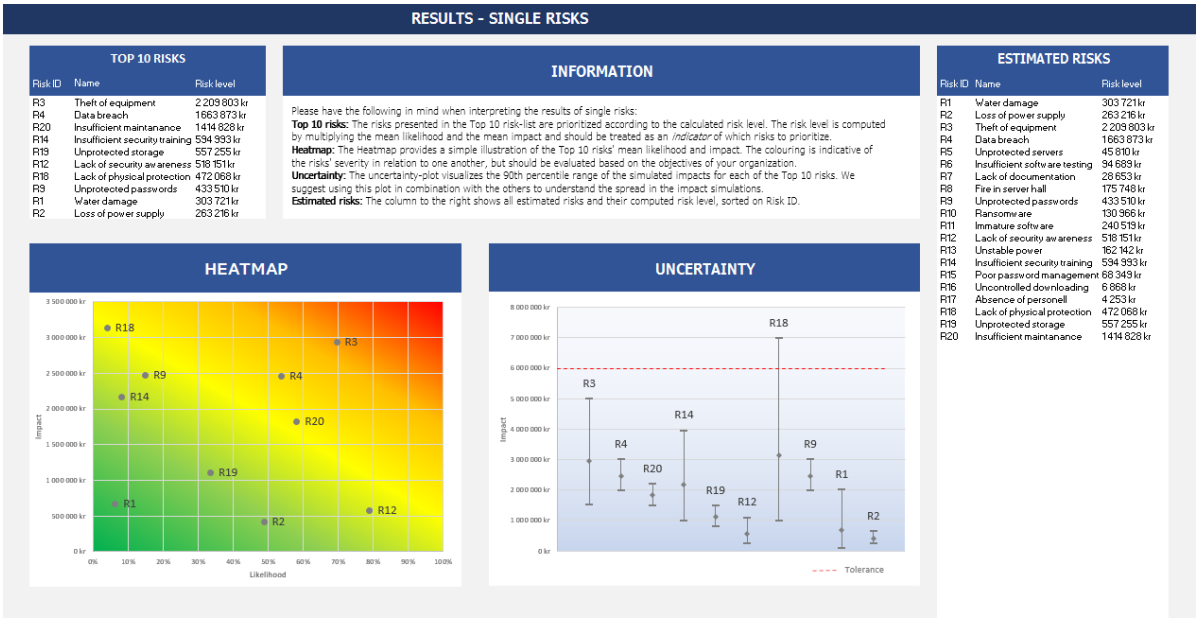



*Figure 29. Results – Single Risks worksheet.*

After having pressed the green *Simulate now button* in the Estimations-worksheet, the MaRiQ tool runs 10 000 simulations and makes computations based on the provided estimates. How this is done will be outlined in the coming section, *8.2.2 Statistical considerations*. When the program has run the simulations and completed the computations, the user is forwarded to the Results – Single Risks worksheet, as shown in Figure 29. This worksheet consists of five main sections. One of these is the information section, which is shown at the top-centre of the figure. Here, the different visualisations in the worksheet are described and suggestions are given on how to interpret the produced tables and graphs.

To the right of the information section, in the top right corner, a second section is visible called *Estimated risks.* Here, all risks that were entered in the Estimations-worksheet are listed with ID, name, and calculated mean expected loss. This section can be used to easily retrieve the ID of each risk and to see their respective simulated risk level.

The remaining three sections aim to provide different perspectives of the results for the assessor. In the top left corner, the *Top 10 Risks* section is visible. Here, a sorted list of the ten risks with the highest computed mean expected loss during the simulations is presented. The list offers an indication of which risks to prioritize, even though the stated value should be treated with caution since it is simply the averaged result from the simulations.

The *Heatmap* section, in the bottom left corner, is based on the mean likelihood and mean impact of the top 10-prioritized risks. The background of the heatmap is coloured in green, yellow and red, aiming to indicate the severity of the risks in relation to one another. If the objective of the organization is to prioritize according to expected loss, risks in the top right corner are more likely to be critical than risks in the bottom left corner, since they have a higher mean impact and mean likelihood. The heatmap is also useful if the organization

wishes to prioritize risks according to impact or likelihood since it is possible to distinguish which risks have a higher mean impact and are more likely to occur.

The fifth and last section in the Results – Single Risks worksheet is called *Uncertainty* and is placed in the bottom right corner. Each line in the graph correspond to one of the top 10-prioritized risks. The length of each line represents the interval within which 90% of the simulated impacts fell. In addition, each risk has a small marker which illustrates the mean of all simulated impacts. If looking at, for example, risk R18 it is possible to see that 90% of all simulations generated impacts between 1 million and 7 million. These impact ranges aim to reveal the spread of the output distribution of the impact and thereby complement the previously described information by showing the uncertainty of the results.

### 8.2.1.4 Results – Total Risks


*Figure 30. Results - Total Risks worksheet.*

Having studied the single risk picture of the organization, the MaRiQ tool also provides a worksheet where the user can overview the total risk situation. Results – Total Risks, as the worksheet is called, provides a cumulative frequency plot, in our tool called impact exceedance graph. The impact exceedance graph visualizes the combined risk impact and an information section giving guidance on how to interpret the results.

As shown in Figure 30, there are two curves in the graph. The blue curve represents the simulated outcomes of the total risk impact and should be interpreted as the probability of the impact exceeding a specific value. We can, for example, see that there is an 40 % probability that the impact exceeds approximately 10 million SEK. If the user is interested in the specific probability of the impact exceeding a certain amount, it is possible to make use of the function in the blue ribbon under the graph. As visible in Figure 30, the user can enter an impact in the white textbox and get the corresponding probability in return. In the same blue ribbon, it is also possible to see the expected total impact. The red curve in the graph

represents the total risk tolerance, as stated by the user in the Estimations-worksheet. Having the blue and the red series in the same graph, it is possible for the assessor to evaluate whether the total risk picture is above or below the stated tolerance.

### 8.2.2 Statistical considerations of the MaRiQ tool

As we learned in section 2.4 *What are the gains of quantitative risk analysis?,* one of the main advantages of using quantitative measures in risk management is that it enables the use of statistics. Statistical computations play a central role in our developed tool and it is, therefore, necessary to describe these considerations in detail.

#### 8.2.2.1 From estimates to distributions

In the MaRiQ tool, impact and likelihood are estimated as ranges in order to capture the uncertainty of the assessor as well as the natural variability of the impact and likelihood. We have chosen not to separate uncertainty and variability in our simulations due to the fact that such a separation would require additional time and effort from the assessor, as described in section *5.4 Variability and uncertainty*. Thus, the MaRiQ tool simulates the *total uncertainty* of the assessment. This decision was based on the fact that many of the surveyed consultants required the model to be easy to use and time-efficient, and that the use of total uncertainty still produces reasonable estimates. Yet another decision made relating to range-estimates, was to use the confidence-level 90 % in the simulations. This means that the assessor should provide estimates of likelihood and impact within which he or she is 90 % certain that the true value lies.

To make calculations based on range-estimates, we needed to implement a method that could handle the fact that there is no single value representing the estimate. Our solution to this problem was to use Monte Carlo simulations. As described in section *5.5 Monte Carlo Simulations,* the Monte Carlo engine takes a distribution as input to randomly generate values. Therefore, we needed to specify the type of distribution for each of the estimated risk-factors: impact and likelihood.

Starting with the impact, we chose to model total uncertainty as a lognormal distribution. The main reason why we chose the lognormal distribution, and not any other of the ones presented in section *5.2 Distributions,* is that the lognormal distribution cannot generate illogical negative amounts, but has a tail to the right that allows for the possibility of extreme large outcomes. Therefore, the lognormal distribution is often a realistic representation of various amounts of loss. Another advantage that motivates the use of the lognormal distribution is the fact that it only requires the assessor to estimate two values – the lower bound (LB) and the upper bound (UB) – while others, such as the triangular distribution, requires three.

A reasonable question to ask at this point is how we go from estimations of LB and UB to a distribution? The answer is that we make use of two basic features of distributions presented in section *5 Statistical aspects of risk management modelling.* First, we utilise the fact that the

assessor provides a 90 % confidence interval of his or her estimate. The 90 % confidence interval tells us that there is a 5 % chance that the true answer lies above the UB and likewise, a 5 % chance that it lies below the LB. Second, we make use of the statistical measures mean and standard deviation of the distribution to find its shape, which can be calculated using the stated LB and UB. Figure 31 illustrates the constructed 90% confidence interval based on the estimated LB and UB for the lognormally distributed impact. For those interested, a detailed description of these calculations can be found in *Appendix E*.

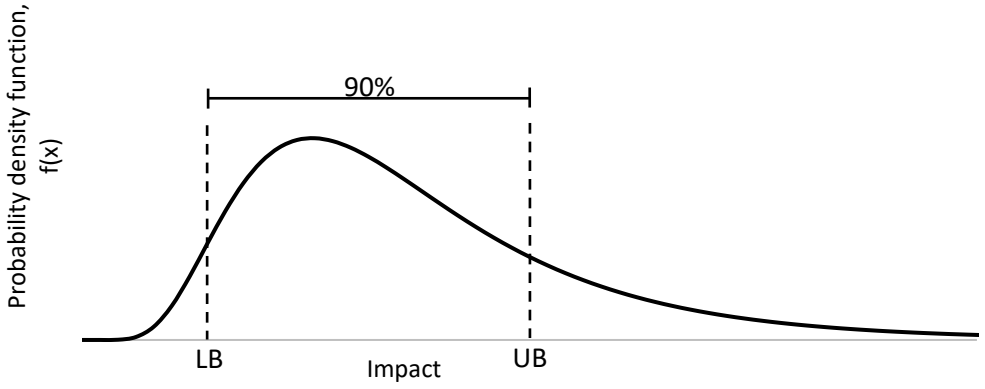



*Figure 31. 90% confidence interval for the lognormally modelled impact with stated upper and lower bound.*

An effect of choosing the lognormal distribution for modelling total uncertainty is that the importance of narrowing down the interval to a 90 % confidence level increases. A very large interval will result in a lognormal distribution that has a greater dispersion, which will significantly increase the probability of extreme events. This can conceptually be understood by keeping the mean fixed and increasing the standard deviation, as shown in Figure 32. As is shown, the distribution obtains a peak with a decreased spread and a thicker tail to the right when the standard deviation increases. Describing how large intervals affect the shape of the distribution in detail is complex since the mean and standard deviation calculations of the lognormal distribution include logarithms of the lower and upper bound. The bottom line here is that a very large interval causes the lognormal distribution to be highly dispersed, which significantly increases the probability of extreme events. Since this will in turn generate results that may seem unrealistic, it is important for the assessor to be aware of this property of the lognormal distribution.

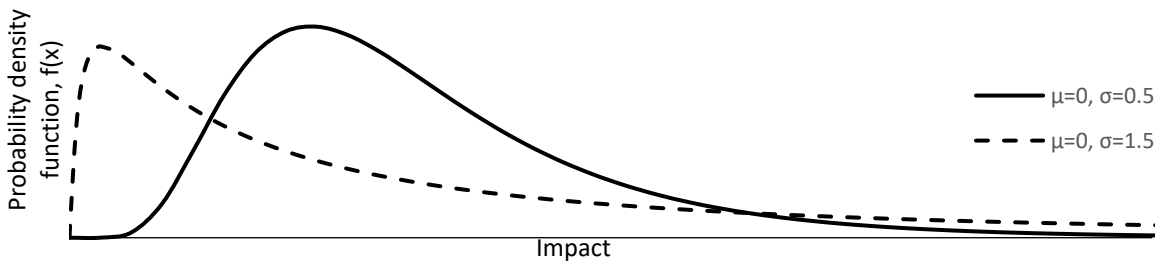



*Figure 32. Probability density function for lognormal distribution with fixed mean and altered standard deviation.*

Now that we understand how the impact is modelled, we turn to the second component of risk: likelihood. As stated in section *5.2 Distributions*, beta distributions can be used to model probabilities such as the likelihood of an event. Since it is rather complex to obtain a beta-distribution based on an interval, we have chosen not to use them in our tool. Neither, we have no reason to believe that the likelihood should be modelled as a lognormal distribution – as is the case with risk impact – since it is illogical to think that the variability of the likelihood allows for extreme values. Instead, we find it reasonable to model the likelihood as a uniform distribution, since it could be argued that each possible likelihood-value within the 90 % confidence interval are equally likely to occur.

In contrast to the lognormal distribution, the uniform distribution could be modelled without a confidence interval by simply estimating the maximum and minimum value of the distribution. However, we believe that changing between different confidence levels for impact and likelihood would be confusing for the assessor. Thus, we have chosen to use a 90 % confidence interval for the likelihood uniform distribution as well. How we find the shape of the uniform distribution of the likelihood based on the LB and UB is illustrated in Figure 33 and further outlined in *Appendix F*.

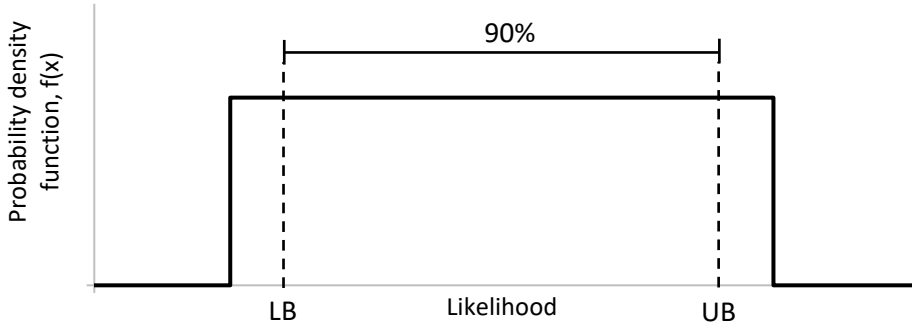



*Figure 33. 90% confidence interval for the uniformly modelled likelihood with stated upper and lower bound.*

#### 8.2.2.2 Total risk simulations

How then, are these distributions applied in our tool? To simulate the total risk impact, we have made use of Hubbard and Seiersen's (2016) comprehensive work on total risk picture modelling to produce a cumulative frequency plot. The procedure described here should therefore first and foremost be referenced to them.

After the user has provided range-estimates for each of the identified risks, the MaRiQ tool runs 10 000 Monte Carlo simulations based on the distributions of the estimates. The purpose of the simulations is to evaluate whether the listed risks occur or not and, in that way, generate a total risk picture of the organization.

To evaluate whether the risks occur or not, we make use of statistical properties of random numbers. First, the tool randomly draws a number from the estimated uniform likelihood distribution, let us call this number $R_{est}$. The drawn number $R_{est}$ is thereafter compared to a

randomly generated number between 0 and 1, also from a uniform distribution. We have chosen to refer to this number as $R_1$. If $R_{est}$ is greater than $R_1$, the event is treated as none-occurring and the impact for that risk in that simulation is set to zero. On the other hand, if $R_{est}$ is less than $R_1$, we model the risk in this simulation to occur and proceed to simulate the impact of the risk.

The motivations behind this method of evaluating risk occurrences are the following: Let us say that we randomly draw a number from the estimated likelihood distribution of 0.15 (15%). We compare this number to another randomly generated number between 0 and 1, for example, 0.12. Since the distribution of the range 0 to 1 is uniform, there is a 15 % chance that the generated number will be less than 0.15. Hence, it is the same probability that the randomly generated number will fall within the range of 0 to 0.15, as is the probability of the risk occurring. The number 0.12 is less than 0.15 and it is, therefore, reasonable to model the risk as occurring. In the same way, we can say that there is an 85% chance that the risk will *not* occur, which corresponds to the chance of drawing a random number in the range of all numbers greater than 0.15 and smaller than 1.

Assuming that the risk was modelled as occurring, the MaRiQ tool proceeds to modelling the impact of that risk. To simulate the impact of a given risk, the tool generates a new random number, $R_2$, to use as input to the lognormal inverse cumulative distribution function. This inverse function uses $R_2$ to obtain an impact from the estimated distribution, as shown in Figure 34. How this works statistically is outlined in detail in section *5.5 Monte Carlo Simulations.*

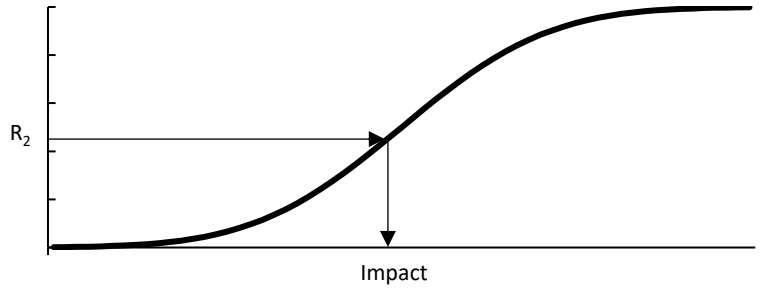



*Figure 34. Illustration of how the generated random number, $R_2$, is used to draw an impact from a given cdf.*

In summary, the whole process of simulating the total risk picture can be described as in Figure 35. We have chosen to refer to the results from the simulations of all risks once as a *scenario.* Hence, Figure 35 shows the procedure of one scenario and in the MaRiQ tool, this is repeated 10 000 times.

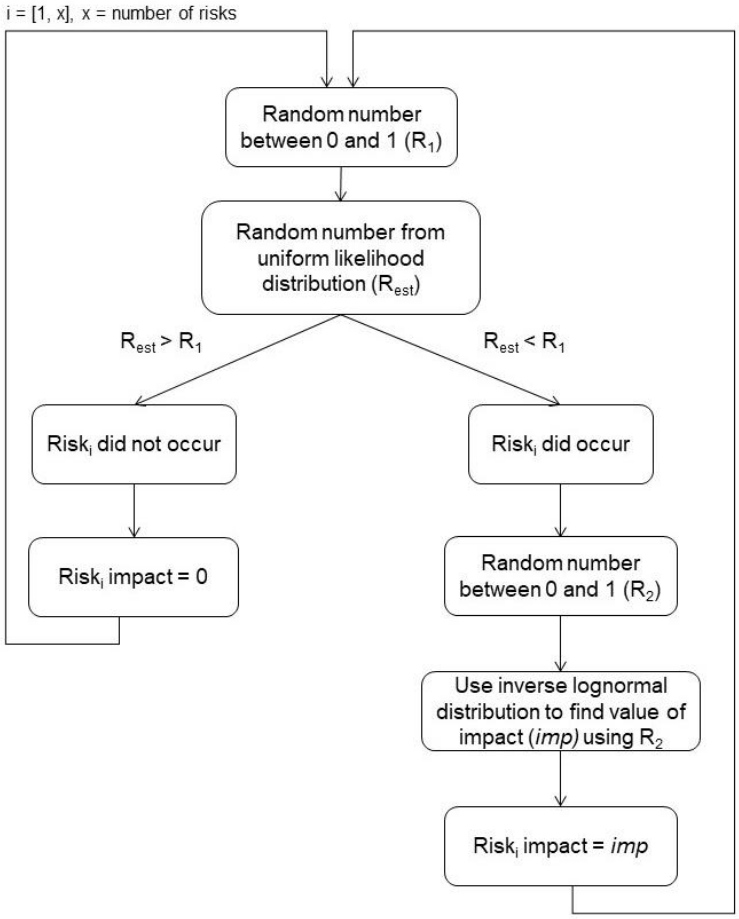



*Figure 35. The risk scenario Monte Carlo simulation process.*

The output of these simulations is a matrix with as many rows as simulations and as many columns as the number of risks listed. Every entry in the matrix corresponds to the simulated impact for one risk in one scenario. An illustration of the matrix for an assessment including three risks: A, B, and C, is shown in Table 5.

*Table 5. Resulting matrix from Monte Carlo simulations of total risk occurrences*

| | Simulated impact (SEK) | | | |
|---|---|---|---|---|
| | Risk A | Risk B | Risk C | Sum |
| Scenario 1 | 0 | 537168 | 0 | 537168 |
| Scenario 2 | 0 | 0 | 238978 | 238978 |
| Scenario 3 | 27556 | 0 | 405231 | 432787 |
| …. | …. | …. | …. | … |
| Scenario 10000 | 0 | 0 | 0 | 0 |

The matrix is used to evaluate the total impact of the occurring risks in each scenario. This is done by summarizing all values in each scenario, as shown in the rightmost column. Based on the maximum value of all summarized impacts, an array with 120[1] evenly distributed values from zero to the maximum is set up. For each of the 120 levels, we calculate the percentage of the simulated total impacts that exceed the specified level. These computations are thereafter used to produce a histogram which is the basis for the Total Risks curve, as shown in section *8.2.1.4 Results – Total Risks*.

#### 8.2.2.3 Single risk simulations

While the total risk simulations aim to evaluate whether risks occur at all, the single risk simulations treat every risk as occurring. The purpose of the single risk simulations is to evaluate the expected loss for each risk, and thereby enabling prioritization and evaluation of the risk components likelihood and impact.

A simulation in the case of single risks means that a likelihood is randomly drawn from the risk's uniform likelihood distribution and likewise an impact from the risk's lognormal impact distribution. The generated values are thereafter multiplied to obtain the expected loss.

In the MaRiQ tool, the values retrieved during these simulations are stored in three matrices: a likelihood matrix, an impact matrix, and an expected loss matrix. The number of columns in the matrices corresponds to the number of risks and the number of rows equals the number of simulations. As previously stated, the number of simulations is set to 10 000 in the MaRiQ tool. Table 6 shows an example of what the impact matrix may look like after simulations of three risks: A, B, and C. The likelihood matrix and the expected loss matrix have the exact same structure.

*Table 6. Example of a matrix containing simulated impact values in the MaRiQ tool*

| | Simulated impact (SEK) | | |
|---|---|---|---|
| | Risk A | Risk B | Risk C |
| Scenario 1 | 55836 | 537168 | 235642 |
| Scenario 2 | 82365 | 501122 | 310856 |
| Scenario 3 | 27556 | 618523 | 162338 |
| …. | …. | …. | …. |
| Scenario 10000 | 64589 | 45836 | 256987 |

[1] 120 is chosen simply because it gives enough data points to create a smooth graph.

The three matrices (likelihood, impact and expected loss) are the basis of the single risk results. The data in the matrices are used for computations of statistical measures and visualization of the output distributions. In order to provide a prioritization of the risks, the MaRiQ tool computes the mean of the expected loss simulations for each risk and sorts the risks in descending order, based on the mean expected loss. The mean is also computed for every risk's likelihood and impact values and plotted in the Heatmap. In addition, the likelihood and impact simulations are used to show the spread of the output distribution, as shown in the Uncertainty-graph in section *8.2.1.3 Results – Single Risks*.

## 8.3 Review of client-case

To evaluate whether the MaRiQ model meets the requirements stated in section *6 Model requirements*, we conducted a two-sessional workshop with one of Nixu's customers. The first session lasted for three hours and was conducted on the 15th of May 2019. Apart from us and our supervisors, five employees participated on the customer's part. The customer was active within the banking industry and had an interest in getting to know more about quantitative approaches to risk management, even though their current practices were qualitative.

The first hour of the workshop was spent presenting what quantitative risk analysis is and how the MaRiQ model and its accompanying tool work. During the remaining two hours we followed the MaRiQ process to carry out the analysis (see Figure 25 section *8.1 Description of the MaRiQ Model* ). Before the workshop we had asked the customer to prepare all necessary input, which means that they had already assembled a working group, defined the object of analysis, established a timeframe, identified risks and decided on their total and single impact tolerance. We thereafter followed the model step by step and used the tool to perform the simulations, make the necessary calculations and to visualize the results.

During the workshop we made several interesting findings. First, we noticed that some participants found it difficult to think about risk in quantitative terms. They expressed that it was new to them to express the risks as a percentual likelihood and a monetary impact and that it was somewhat tricky to find reasonable estimates. Even though they found it hard, they all stated that it seemed like a very viable method and that, with training, it would be easier to come up with accurate numbers. They also stated that in comparison to current qualitative processes, the MaRiQ model was perceived as more accurate since it is possible to review the stated monetary impact and likelihood.

Another finding we made relating to expressed difficulties was that the term *expected loss* caused confusion. Some participants interpreted this as a measure of the predicted cost of each risk, when it should really be understood as an indication of the risk level. Moreover, the participants stated that it was not entirely clear how the expected loss related to the single and total impact tolerances. They did appreciate however, that the tool visualised tolerances which made it easier to understand which risks to prioritize.

A third finding from the workshop was the importance of stating a 90 % confidence interval. As described in section *8.2.2.1 From estimates to distributions,* very large intervals can cause the lognormal distribution to be highly dispersed. This will increase the probability of including extreme values in the simulations, which will in turn have a large impact on the results. During the workshop, the customer provided an impact estimate with a ratio of 1:1 000 000, which made the results seem unrealistic. After discussions it stood clear that the customer had not really provided a 90 % confidence interval, and that the interval needed to be narrowed down.

To conclude our findings from the first workshop session, we learned that the MaRiQ model is a realistic and viable alternative to current qualitative processes, even though it was not entirely easy for the customer to fully transition from qualitative to quantitative ways of thinking. The participants stated that the MaRiQ model was relatively easy to understand and to start using and that the results were sufficient for future decision making. Moreover, we learned that the workshop leader plays a key role in making sure that the assessor understands the different features of the model, such as expected loss and 90 % confidence interval.

The second workshop session took place on the 17$^{th}$ of May, two days after the first one. During this session, we posed questions to the participants aiming to capture how well the MaRiQ model fulfilled the stated requirements. The findings from this evaluation will be further discussed in the coming section, *9 Discussion*, where we will also elaborate on how the model can be improved in the future.

# 9. Discussion

In this thesis, we aimed to create a quantitative risk management model, suitable for use at the cybersecurity consultant firm Nixu. The created model, MaRiQ, was developed based on user and literary requirements and on already established risk management frameworks. In this section, we will reflect upon our work by evaluating how well the MaRiQ model fulfills the stated requirements. Moreover, will provide suggestions on how our developed model and its accompanying tool can be furthered in the future.

## 9.1 Evaluation of requirements

Having presented the final result of our work, it is in order to reflect upon the process and discuss how well we managed to meet the stated requirements. Figure 36 shows a summary of all user requirements (UR), literary requirements (LR) and additional requirements (AR) as stated in section *6 Model requirements*. On the coming pages, we will discuss how we have tried to meet these requirements and also outline how the customer perceived the model with regards to the same. The customer view-points were collected during the second workshop session, as described in section *4.3.2 Client-case*.

| | |
|---|---|
| *UR 1* | **Communicative** |
| *UR 2* | **Practical** |
| *UR 3* | **Prioritized** |
| *UR 4* | **Scientific** |
| *LR 1* | **Consistent** |
| *LR 2* | **Adaptable** |
| *AR 1* | **Compound** |
| *AR 2* | **Balanced** |

*Figure 36. Requirements for the risk management model.*

### 9.1.1 Communicative

*The risk management model must generate results that are easy to communicate to management and organization.*

Our ambition was to make the MaRiQ model communicative by enabling flexible presentation forms of results that can be adapted to suit the receiver. Therefore, the MaRiQ model does not explicitly state *how* the assessor should present the results of the assessment, but simply that prioritized risks, the total risk picture and the uncertainty should be visualised. The MaRiQ tool provides examples of how results can be presented using tables and graphs. The customer participating in the workshop expressed that the MaRiQ tool was visually appealing and that it provides sufficient information for communicating risks on a general level with management and organization. They did state, however, that some developments could be made in order to make the tool even more applicable to their organization. A few such examples were that they desired a tolerance level for the expected loss, the possibility to evaluate risks based on loss forms (such as reputation and legal expenses) and to see more details about the output distribution of the simulated values.

Another feature we implemented in MaRiQ to make the model communicative is that it proposes two perspectives on how to evaluate risks: the total and single risk picture. The total risk picture enables the assessor to quickly get an overview of the risk situation, whereas comparisons of single risk impacts and expected loss provide indications of which risks that are most important to prioritize. This double-edginess of MaRiQ is perhaps the biggest contribution of this model to the field of quantitative cybersecurity risk management since we have not yet found any existing model that simultaneously supports the single and total risk perspective. The customer confirmed that it was valuable to have both risk perspectives and explained that the total risk picture was very appreciated in their organization since they had no way of knowing how much money to allocate for total risks in current qualitative processes.

To make the model communicative, we chose to present relatively few and simple statistical measures to the user in the MaRiQ tool. Still, the customer expressed that the results were already better than qualitative counterparts since it was perceived as easier to relate to a monetary consequence than for example *yellow* or *red*. The customer also expressed that it was more sensible to talk about consequences on a continuous monetary scale, than as a certain impact category, since the mitigations will always be evaluated in monetary terms.

In summary, the customer experienced MaRiQ to be a communicative tool since it provides two perspectives of the risk picture which facilitates the process of providing relevant information to management and organization. The MaRiQ tool was perceived as an intuitive and visually pleasing software that provided sufficiently elaborate results. The customer did state, however, that the tool could be further developed to suit organizational purposes better.

### 9.1.2 Practical

*The risk management model must be practical, in the sense that it is time-efficient and easy to use.*

To make MaRiQ practical, we introduced several features to facilitate the implementation of the model. MaRiQ is for example based on the already well-established ISO 27005 framework which should make it easier for people working with cybersecurity risk management to understand and use the model, since they are likely already familiar with ISO 27005. The customer stated that the model was very viable and that there were really no obstacles to start using MaRiQ since they experienced that the knowledge needed is basically the same as in qualitative processes. Some of the workshop participants did express that it was troublesome to find accurate estimates. Unfortunately, we did not have time to go through the suggested calibration techniques and decomposition strategies, as presented in section *7.1.2 Estimation of risk impact and likelihood* during the workshop. Our hope is that these practises will make the model even more time-efficient and easy to use. Even without these techniques and strategies however, the customer expressed that MaRiQ was no more time-consuming than current qualitative practices.

One feature that we believe contributes to the perception of MaRiQ as time-efficient and viable, is the fact that there is a supporting tool. The MaRiQ tool was developed with the term practical in the centre. An example of how this applies is the fact that it was created in Excel using VBA. It is reasonable to believe that Excel is more accessible and easier to use for the larger masses, than optional software or programming languages such as R, Python or Java. Our hope is that the target group of our model will not have to install any new software or go through complicated tutorials to start using the MaRiQ tool. Yet another practicality of our developed tool, is that the user does not need to deal with problems of simulations and cell references since the functionality of the model is solely based on VBA-scripts. This means that all computations and modelling are done in the background while the user can focus on what is really important – namely analysing the results.

Another example of how we have prioritized practicality in the MaRiQ tool is that we chose to model the impact and the likelihood using distributions that require only two input values: the upper and the lower bound. We could have used other distributions to model the risks, such as triangular, but since the triangular distribution would require more time and effort from the user we chose not to use it in favour of the less complex lognormal and uniform distributions. Despite our efforts to reduce the number of estimates, the customer participating in the workshop stated that they would not have had anything against providing more input-values to the model. Important to note, however, is that this customer was relatively mature when it comes to risk management. In order to draw any general conclusions regarding the number of input-values we would therefore need to expand the workshop to also include less mature organizations.

### 9.1.3 Prioritized

*The risk management model must provide prioritization of the analysed risks.*

To enable the assessor to prioritize among risks, we implemented a number of features in the MaRiQ model and tool to facilitate ranking. One of these features is the fact that the tool provides a sorted list of the top-ten risks that obtained the highest mean expected loss. Another example is that the model allows the user to prioritize based on any desired feature, and in the tool, it is for example possible to prioritize risks according to the average impact or likelihood by studying the Heatmap. A third feature is that MaRiQ enables the organization to see if they need to prioritize risks at all, through the total risk impact graph.

The customer who tested MaRiQ stated that the tool provides a good baseline of which risks to prioritize, but that more measures are needed to decide on prioritization. Cost of mitigations was one such measure and risk description another. The customer also desired that the tool would enable the assessor to dive deeper into the results. This could for example be done by presenting more details about the output distribution of the simulated risks, or by allowing the user to prioritize according to different types of risks. One such example that we mentioned during the workshop was Freund and Jones' six forms of losses (as presented in Table 3 in section *7.1.2 Estimation of risk impact and likelihood*), which was warmly welcomed by the customer.

An issue concerning the MaRiQ tool that was mentioned during the second workshop session, was that some assessors might put too much faith in expected loss as a measure when risks are presented in a top 10 list. This is an issue that should not be overlooked since it is necessary to also study the averaged impact and likelihood as well as the uncertainty to make sound decisions based on the MaRiQ tool. This discussion is closely related to the topic of workshop setup, where it is crucial that the workshop leader clearly explains how the different graphs should be interpreted, why they are important and what expected loss actually is.

### 9.1.4 Scientific

*The risk management model must be scientific, in the sense that it is logical and use proper math.*

There are several features of MaRiQ motivating why it is scientific. First of all, MaRiQ bases its simulations on values from ratio scales which enables the use of proper math and statistical computations. Moreover, MaRiQ reflects the total uncertainty of the analysis which provides a more nuanced perspective of the results. The uncertainty and variability are captured during the initial phase of the process through range-estimates, as well as in the final stages where the total uncertainty is communicated to the recipient – in our developed tool through an uncertainty-plot. The simulations themselves also contribute to MaRiQ's scientific grounds, since the results are based on numerous statistical outcomes and not only subjective point estimates.

The MaRiQ tool is also scientific in the sense that the input to the Monte Carlo engine is distributions, as is the output produced during the simulations. This avoidance of using single value-estimates increases the credibility of our model, which in turn increases the chances of accurately forecasting potential consequences of risks that the organization faces. One potential drawback of MaRiQ's scientific grounds that was mentioned during the workshop, was that users might become overconfident in the results. This means that they might for example believe that the averaged expected loss provides the full risk picture, when in reality it is just an indication of the risk severity. As in the case of prioritization, it is vital that the person introducing MaRiQ is open about its prospects and clearly outlines how the model should be used and the results interpreted.

### 9.1.5 Consistent

*The risk management model must be consistent, meaning that it produces similar results regardless of the group or person performing the assessment.*

To meet the requirement of consistency, we tried to the best of our ability to create a clear model description that allows for as little confusion as possible. By having eleven clearly outlined and defined steps that the user should follow sequentially every time the model is used, we believe that the chances of producing similar results increase. The MaRiQ tool also contains explicit information on every worksheet explaining what should be done and how it should be carried out, which is also meant to increase the consistency. Moreover, the MaRiQ model and tool strongly encourages the user to document the reasoning behind each estimate, which should also make the model more consistent since it enables critical review of the estimates.

The customer who tested our model expressed that in relation to qualitative practices, MaRiQ increases consistency by not allowing the assessor to freely reposition risks. Using the qualitative risk matrix, it is for example possible to move risk X from *red* to *yellow* if it does not suit the organization to treat X as a red risk. This change in position was, according to the customer, not unheard of. In the quantitative analysis, on the other hand, it is not possible for the assessor to tamper with risks in the same way since it is very hard to pre-calculate what the simulated outcome will look like. Moreover, estimates of impact and likelihood are no longer subjective judgements inside someone's head, but explicitly stated monetary and percentual units.

Important to note here, however, is that despite our attempts to create a consistent risk management model it is very hard to create a fully coherent process. Every person has his or her own way of thinking and therefore, even the results of the quantitative assessment will most likely differ depending on the assessor. Despite thorough documentation, expert calibrations and explicitly stated estimates, the requirement of consistency is hard to fully reach.

### 9.1.6 Adaptable

*The risk management model must be applicable to a variety of organizations and situations.*

MaRiQ is meant to be an operational cybersecurity risk management instrument that can be broadly applied, irrespective of the type of organization at stake. Even though the model was developed for cybersecurity purposes, we realized from the workshop-feedback that there are really no hinders for using it in industries where information technology is not the primary area of interest.

MaRiQ is adaptable in the sense that the model description allows for a variety of set-ups. It is for example up to the user to define the timeframe, currency, amount of risks analysed, number of simulations and which statistical measures to compute. Moreover, the results can be visualised in a variety of ways and the MaRiQ tool provides examples of how to communicate risks through graphs and heatmaps.

The requirement of adaptability is necessary since our target organization, Nixu, is working with a variety of customers. It is important to note, however, that this flexibility of usage also comes with a downside. Since the directions and recommendations are relatively vague, it could be argued that MaRiQ is harder to implement than other, more strictly specified risk management processes. Moreover, it is likely that each and every target organization have different needs of the model and that MaRiQ's relatively high-level results will therefore not suit everybody. This potential weakness was confirmed during the workshop when the customer expressed that they desired more elaborate results that could be used to dig deeper into each risk. At the same time, they did state that MaRiQ provides results that are sufficient for future decision-making.

### 9.1.7 Compound

*The risk management model should be based on already existing risk management methods/models/frameworks/standards.*

MaRiQ would not have existed without its predecessors. The model is based on and inspired by a number of previous methods, models, standards and frameworks such as the ISO 27005-standard, Freund and Jones FAIR-model, Hubbard & Seiersen's risk management model, The Open Group's requirements for risk management models, the COSO ERM framework and Vose's statistical considerations for risk management. One workshop-participant had previously come across other quantitative models for evaluating risks and stated that MaRiQ seemed to have captured relevant parts of these.

### 9.1.8 Balanced

*The risk management model must be balanced with regards to simplicity and complexity.*

Risk is a complex phenomenon that is not easy to model in a simple way. The ambition of MaRiQ is to be complex enough so that the results are accurate and valid, while still being

easy to use so that organizations find it reasonable to switch from qualitative to quantitative processes. Therefore, relatively complex features have been implemented (such as range-estimates and risk simulations), but always to a degree that we considered reasonable to the user.

According to the customer who tested our model, MaRiQ does not need to be more complex. At the same, the customer expressed that in an optimal version it would be possible to get more information about each simulated risk in the tool. In general, the customer appreciated the simplicity of the model and stated that it is better to approach organizations with an understandable and appealing model since there is often an initial reluctancy towards risk management.

## 9.2 Future work

In this study, we have provided motivations as to why the cybersecurity community should transition from qualitative to quantitative approaches to risk management. We have also presented our own developed quantitative model, MaRiQ, and described how it was perceived a real-life client-case. Even though the model was appreciated by the customer who tested it, there are of course numerous ways in which MaRiQ can be improved. In this section, we will outline ideas and suggestions for future work that can be done in order to further the model.

Before getting into details about possible developments, it is necessary to mention that it is hard to draw general conclusions regarding the usability of MaRiQ since it has only been tested on one organization. In order to fully understand the potentials and deficiencies of the model, one would need to conduct additional workshops with more and other types of organizations. A first idea for future work is therefore to test the model on a larger scale, with organizations that have a varying degree of analytical maturity when it comes to risk management.

Another suggestion to further the model is to expand its scope. As of today, MaRiQ only includes three of eight activities in the ISO 27005 framework, as shown in Figure 4. The two ISO-activities that we consider especially relevant to handle are *risk identification* and *risk treatment.* Since the identified risks constitute the basis of the rest of the assessment, it is crucial that the risks are accurately scoped and well-defined. We have not yet studied how a quantitative risk identification process should be carried out and it would therefore be interesting to evaluate this activity in more depth. Adding risk treatment is another logical expansion of the scope, since it is essential for the organization to evaluate possible mitigations before deciding on how to proceed.

In addition to testing the model on a larger scale and expanding the scope, we have identified a number of minor areas in which the model can be improved. One of these is to widen the literary acquisition. In this thesis, we have chosen to study risk management from a cybersecurity perspective, which means that we have not included literature from other

relevant branches of industry, such as finance or insurance business. It is likely that such a development would provide new and useful insights to the cybersecurity industry. Another potential development of the MaRiQ model is to include risk dependencies. As of today, MaRiQ treats risks as if they were independent from each other, but we suggest that further studies are carried out to examine risk dependencies and how these could be included in the model. Lastly, our study has shown that there is a desire within the cybersecurity community for risk management models that can handle "soft" aspects of risks, such as reputation and competitive advantage. To help organizations estimate these types of risks, we suggest that studies are carried out aiming to provide guidelines on how to estimate softer aspects of risks.

So far, we have outlined suggestions for future work relating to the model itself. There are of course also potential developments to made when it comes to the MaRiQ tool and below, we have outlined some of the areas identified as improvable. We suggest to:

- Use the beta-distribution instead of the lognormal distribution to model the risk likelihood. Doing so, Bayesian statistics would be more applicable since the beta-distribution can easily be updated using prior estimates.

- Implement support for decomposition by allowing the user to estimate the impact of for example Jones and Freund's six forms of losses. We also suggest including visualisation of the decomposed impacts in the Results-worksheets.

- Separate variability from uncertainty in the assessment. This would allow the assessor to identify what part of the imprecision that is caused by the natural randomness of the system and what is caused by the assessor's lack of knowledge. Having such insights would allow the assessor to reduce uncertainty by further measurements.

- Implement mitigations and visualise how risks are affected after the introduction of countermeasures.

- Let the user decide on prioritization-basis. As of now, the MaRiQ tool only provides explicit prioritization based on expected loss.

- Enable switching from likelihood to frequency to manage risks that occur multiple times during the stated time-frame.

To summarize, there are several potential developments that can be made to the MaRiQ model and tool. From the workshop we learned, however, that MaRiQ seems to be a suitable starting point for organizations to initialize the transition from qualitative to quantitative approaches. We hope that MaRiQ can serve as an inspiration for organizations aiming to move towards quantitative risk management and that it can be a springboard from which new developed models can take form.

# 10. Conclusion

The purpose of this project was to create a quantitative risk management model, attuned for the cybersecurity consultant firm Nixu. The three research objectives we aimed to fulfil in this study were:

- To survey available risk management models used within the cybersecurity community,
- To develop a quantitative risk management model, attuned for Nixu and its customers, and
- To produce a software tool that supports the model.

In this thesis, we have presented already existing risk management models, some of which have been integrated into our own developed model. We have also presented the model that we created, MaRiQ, in the form of a flowchart and a model description. Further, we have described the software tool that we developed in Excel to support relevant parts of the MaRiQ model.

Our results indicate that risk management within cybersecurity can and should be performed using more quantitative approaches than what is common practice today. Our developed model, MaRiQ, attempts to meet the needs of the industry by being quantitative and to a large extent communicative, practical, prioritized, scientific, consistent, adaptable, compound and balanced.

From the client-case we carried out, we learned that MaRiQ has the potential of serving as a transition engine from qualitative to quantitative risk management due to the perceived low-threshold to start using it. Although there are several potential developments to be made, we hope that MaRiQ can serve as an inspiration for future quantitative risk management models since it demonstrates the benefits that can be obtained from such approaches.

This thesis has proven that the shift from qualitative to quantitative risk management *is* possible and advantageous in many respects. Yet, it is left to see when the cybersecurity industry will reach the analytical maturity needed to fully take on quantitative approaches to risk management.

# References


Alm, S. E. and Britton, T. (2008) *Stokastik : sannolikhetsteori och statistikteori med tillämpningar*. Stockholm: Liber.

Andersson, H. *et al.* (2011) *Riskanalys*. MSB, www.informationssäkerhet.se.

Bayuk, J. (2018) 'Technology's role in enterprise risk management', *ISACA Journal*, 2, pp. 15–21.

Baze, A. (2014) *Realistic Risk Management Using the CIS 20 Security Controls*. Available at: https://www.sans.org/reading-room/whitepapers/riskmanagement/realistic-risk-management-cis-20-security-controls-37135 (Accessed: 8 March 2019).

Budescu, D. V, Broomell, S. B. and Por, H. (2009) 'Improving communication of uncertainty in the reports of the IPCC', *Psychol. Sci.*, 20(3), pp. 299–308.

Budescu, D. V and Wallsten, T. S. (1985) 'Consistency in Interpretation of Probabilistic Phrases', *Organizational behaviour and human decision processes*, 36(3), pp. 391–405.

Caralli, R. A. *et al.* (2007) *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*. Available at: http://www.sei.cmu.edu/publications/pubweb.html (Accessed: 27 February 2019).

Cecula, A. (1985) 'Consider Alternatives to Formal Risk Analysis', *Government Computer News*.

Center for Internet Security [CIS] (2018) *CIS Controls Version 7*. Available at: https://www.defensis.it/ecms/file/CIS-Controls-Version-7.pdf (Accessed: 18 February 2019).

Clemen, R. T. and Winkler, R. L. (1999) *Combining Probability Distributions From Experts in Risk Analysis, Risk Analysis*. Available at: https://faculty.fuqua.duke.edu/~clemen/bio/Published Papers/28.CombiningDistributions-Clemen&Winkler-RA-99.pdf (Accessed: 1 April 2019).

CORE Security (2019) *What is Red Team Cyber Security*. Available at: https://www.coresecurity.com/content/what-red-team-security (Accessed: 12 March 2019).

Cox, T. (2008) 'What's Wrong with Risk Matrices?', *Risk Analysis*, 28(2), pp. 497–512. doi: 10.1111/j.1539-6924.2008.01030.x.

Curtis, P. and Carey, M. (2012) *Risk assessment in practice*. Available at: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/dttl-grc-riskassessmentinpractice.pdf (Accessed: 14 April 2019).

Dagens Nyheter (2019) 'Serveransvariga om Vårdguiden-haveriet: "mänskliga faktorn"', *Dagens Nyheter*, (20 February). Available at: https://www.dn.se/ekonomi/ansvarig-for-vardguiden-haveriet-manskliga-faktorn/ (Accessed: 15 April 2019).

Dobos, L. (2019) '2,7 miljoner inspelade samtal till 1177 Vårdguiden helt oskyddade på internet', *ComputerSweden*, (18 February). Available at: https://computersweden.idg.se/2.2683/1.714787/inspelade-samtal-1177-vardguiden-oskyddade-internet (Accessed: 4 March 2019).

Drisko, J. and Maschi, T. (2015) *Content Analysis*. Oxford: Oxford University Press. doi: 10.1093/acprof:oso/9780190215491.001.0001.

Dubois, É. *et al.* (2010) 'A Systematic Approach to Define the Domain of Information System Security Risk Management', in *Intentional Perspectives on Information Systems Engineering*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 289–306. doi: 10.1007/978-3-642-12544-7_16.

European Union Agency for Network and Information Security [ENISA] (2006) ‘Inventory of risk assessment and risk management methods’, pp. 1–56. Available at: http://www.enisa.europa.eu/act/rm/files/deliverables/inventory-of-risk-assessment-and-risk-management-methods/at_download/fullReport (Accessed: 4 February 2019).

European Union Agency for Network and Information Security [ENISA] (2019) *Risk Management*. Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management (Accessed: 4 March 2019).

Fenz, S. *et al.* (2014) ‘Current challenges in information security risk management’, *Information Management & Computer Security*, 22(5), pp. 410–430.

Forum of Incident Response and Security Teams [FIRST] (2019) *Common Vulnerability Scoring System SIG*. Available at: https://www.first.org/cvss/ (Accessed: 7 March 2019).

Freund, J. and Jones, J. (2014) *Measuring and managing information risk : a FAIR approach*. Wuman Street, Waltham: Elsevier Science & Technology.

Garrabrants, W. M. *et al.* (1990) ‘CERTS: a comparative evaluation method for risk management methodologies and tools’, in *Proceedings of the Sixth Annual Computer Security Applications Conference*. IEEE Comput. Soc. Press, pp. 251–257. doi: 10.1109/CSAC.1990.143783.

Goel, R., Haddow, J. and Kumar, A. (2018) *Managing Cybersecurity Risk in Government: An Implementation Model*. IBM Center for The Business of Government. Available at: www.businessofgovernment.org (Accessed: 12 February 2019).

Gritzalis, D. and Stavrou, V. (2018) ‘Exiting the Risk Assessment Maze: A Meta-Survey’, *ACM Comput. Surv*, 51(11), pp. 1–30. doi: 10.1145/3145905.

Hagevi, M. and Viscovi, D. (2016) *Enkäter: att formulera frågor och svar*. 1st edn. Lund: Studentlitteratur AB.

Haimes, Y. Y. (2015) *Risk modeling, assessment, and management*. Hoboken, New Jersey: John Wiley & Sons, Incorporated.

Hewitt, J. and Pham, D. J. (2018) ‘Qualitative Versus Quantitative Methods in Safety Risk Management’, in *2018 Annual Reliability and Maintainability Symposium (RAMS)*. IEEE, pp. 1–6. doi: 10.1109/RAM.2018.8463052.

Hubbard, D. W. (2014) *How to measure anything : finding the value of intangibles in business*. 3rd edn. Hoboken, New Jersey: John Wiley & Sons.

Hubbard, D. W. and Seiersen, R. (2016) *How to measure anything in cybersecurity risk*. 1st edn. Hoboken, New Jersey: John Wiley & Sons.

Interviewee 1 (2019). Employee at Nixu Cybersecurity: Interview 19 February.

Interviewee 2 (2019). Employee at Nixu Cybersecurity: Interview 19 February.

Interviewee 3 (2019). Employee at Nixu Cybersecurity: Interview 19 February.

ISO 27005 (2018) *Information technology – Security techniques – Information security risk management (ISO/IEC 27005:2018, IDT), Swedish Standard Institute*. International Organization for Standardiszation & International Electrotechnical Commission. doi: http://dx.doi.org/10.1016/j.actatropica.2009.08.018.

ISO 31000 (2018) *Risk management - Guidelines: SFS-ISO 31000:2018*. International Organization for Standardiszation & Swedish Institute for Standards.

Kahneman, D., Tversky, A. and Slovic, P. (1982) *Judgement under uncertainty : heuristics and biases*. Cambridge: Cambridge university press.

Karabacak, B. and Sogukpinar, I. (2005) 'ISRAM: information security risk analysis method', *Computers & Security*. Elsevier Advanced Technology, 24(2), pp. 147–159. doi: 10.1016/J.COSE.2004.07.004.

Kouns, J. and Minoli, D. (2010) *Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams*. Hoboken, New Jersey: John Wiley & Sons.

Kylén, J.-A. (2004) *Att få svar: : intervju, enkät, observation*. 1st edn. Stockholm: Bonnier Utbildning.

Microsoft (2019) *Microsoft Excel*. Available at: https://products.office.com/en-us/excel (Accessed: 31 March 2019).

Mihailescu, V. L. (2012) 'Risk analysis and risk management using MEHARI', *Journal of Applied Business Information Systems*, 3(4).

Mulvaney, B. (2012) 'Red Teams: strengthening through challenge', *Marine Corps Gazette*, (July). Available at: https://www.hqmc.marines.mil/Portals/138/Docs/PL/PLU/Mulvaney.pdf (Accessed: 1 April 2019).

NIST 800-30 (2012) *Guide for conducting risk assessments: Information Security*. Gaithersburg. U.S. Department of Commerce & National Institue of Standards and Technology. doi: 10.6028/NIST.SP.800-30r1.

Nixu Cybersecurity (2019) *Nixu Corporation*. Available at: https://www.nixu.com/about (Accessed: 16 March 2019).

Ny Teknik (2019) *Här är allt vi vet om 1177-skandalen, Ny Teknik*. Available at: https://www.nyteknik.se/sakerhet/har-ar-allt-vi-vet-om-1177-skandalen-6948869 (Accessed: 15 April 2019).

Online Trust Alliance (2018) *Cyber Incident & breach trends report, The Internet Society*. Available at: https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf (Accessed: 11 February 2019).

Petrie, K., Potter, D. and Ankorion, I. (2018) *Streaming change data capture : a foundation for modern data architectures*. 1st edn. O'Reilly Media, Inc.

Pfleeger, C. P., Pfleeger, S. L. and Margulies, J. (2015) *Security in computing*. 5th edn. Upper Saddle River, NJ: Prentice Hall.

Puget, J.-F. (2014) *The Analytics Maturity Model, IBM Community*. Available at: https://www.ibm.com/developerworks/community/blogs/jfp/entry/the_analytics_maturity_model?lang=en (Accessed: 26 April 2019).

Rychlik, I. and Rydén, J. (2006) *Probability and Risk Analysis*. Berlin, Heidelberg: Springer Berlin Heidelberg. doi: 10.1007/978-3-540-39521-8.

Scarfone, K. and Mell, P. (2010) *The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities*. U.S. Department of Commerce & National Institute of Standards and Technology. doi: 10.6028/NIST.IR.7502.

Slayton, R. (2015) ‘Measuring Risk: Computer Security Metrics, Automation, and Learning’, *IEEE Annals of the History of Computing*. IEEE, 37(2), pp. 32–45. doi: 10.1109/MAHC.2015.30.

Techstore (2013) ‘5 main reasons to use Microsoft Excel in your Business’, (May 21). Available at: https://www.techstore.ie/5-main-reasons-to-use-microsoft-excel-in-your-business/ (Accessed: 31 March 2019).

Teorell, J. and Svensson, T. (2007) *Att fråga och svara: samhällsvetenskaplig metod*. 1st edn. Stockholm: Liber.

Tetlock, P. (2015) *Superforecasting : the art and science of prediction*. 1st edn. New York: Crown Publishers.

The MITRE Corporation (2014) *CWE - Common Weakness Scoring System (CWSS)*. Available at: https://cwe.mitre.org/cwss/cwss_v1.0.1.html (Accessed: 7 March 2019).

The Open Group (2009) *Requirements for Risk Assessment Methodologies*. Technical Guide. ISBN: 1-937218-42-3.

The Open Group (2010) *FAIR – ISO / IEC 27005 Cookbook*. Technical Guide. ISBN: 1-931624-87-9.

The Open Group (2013a) *Risk Analysis (O-RA), Technical Standard*. Open Group Standard. ISBN: 1-937218-41-6.

The Open Group (2013b) *Risk Taxonomy (O-RT), Version 2.0*. Open Group Standard. ISBN: 1-937218-00-3.

The Open Group (2018) *Open FAIR Risk Analysis Process Guide*. Open Group Guide. ISBN: 1-947754-06-5.

Vose, D. (2008) *Risk analysis : a quantitative guide*. 3rd edn. Chichester: Wiley.

Wheeler, E. (2011) *Security risk management : building an information security risk management program from the ground up*. Amsterdam: Syngress.

Winterfeld, S. (2016) *The Cybersecurity Canon: How to Measure Anything in Cybersecurity Risk*. Palo Alto Networks. Available at: https://researchcenter.paloaltonetworks.com/2016/12/cybersecurity-canon-measure-anything-cybersecurity-risk/ (Accessed: 20 March 2019).

Wolke, T. (2017) *Risk Management*. Berlin: De Gruyter Oldenbourg.

World Economic Forum (2018) *The Global Risks Report 2018 13th Edition Insight Report*. 13th edn. Geneva: World Economic Forum. Available at: http://wef.ch/risks2018 (Accessed: 11 February 2019).

Zetter, K. (2009) *Senate Panel: 80 Percent of Cyber Attacks Preventable*. Available at: https://www.wired.com/2009/11/cyber-attacks-preventable/ (Accessed: 11 February 2019).

# Appendix A: Interview questions

*Syfte med intervjuer:*

- Att förstå hur cybersäkerhetskonsulter uppfattar nuvarande riskbedömningsmodell(er) för att utvärdera informationssäkerhetsrisker, både i positiv och negativ bemärkelse samt
- Att upprätta en kravspecifikation för den anpassade modellen

*Intervjufrågor:*

- Hur skulle du kort beskriva din roll på företaget?
- I vilket/vilka sammanhang kommer du i kontakt med riskbedömningar?
- Kan du beskriva hur en risk management (riskhanterings-) process (hos kund) generellt kan se ut?
    - Vilka aktörer är involverade?
    - Har alla tillräcklig kunskap?
    - Har ni tillräckligt med tid?
- Vilken riskbedömningsmodell/metod använder ni idag?
    - Hur används modellen/metoden?
- Vilken kunskap / vilka personer behövs för att kunna genomföra riskbedömningen?
- Vad ser ni för fördelar med att arbeta med er metod?
- Vad ser ni för nackdelar med den?
- Hur uppfattar ni att kunderna upplever modellen/metoden?
- Vilka är de största bristfaktorerna i nuvarande processer? *Information? Data? Kunskap? Tid?*
- Vilka är de viktigaste faktorerna för en lyckad riskbedömningsprocess? *Data? Kunskap? Tid?*
- Vad skulle en optimal modell innehålla som dagens modell inte gör?
- Vilka krav vill du ställa på Nixus riskbedömningsmetoder? *Är det exempelvis viktigt att metoden är snabb? Modern?*

# Appendix B: Online survey


Uppsala universitet

## Faktorer för lyckade riskbedömningar

**Tillgänglig** 2019-02-13 – 2019-03-31
**Kontaktperson** Elin Carlsson, verksam vid Insitutionen för Informationsteknologi

Denna enkät är utformad för att fånga den svarandes uppfattning kring faktorer som är viktiga i en bra riskbedömningsmetod. Enkäten kommer att användas i ett examensarbete som genomförs på Nixu under våren 2019 av två studenter på Civilingenjörsprogrammet System i Teknik och Samhälle vid Uppsala universitet.

För varje skalfråga nedan, ange dina preferenser kring hur en optimal riskbedömningsmetod ska vara utformad enligt dig. Utgå från följande frågeställning när du besvarar skalfrågorna:

Hur viktigt är det för dig att riskbedömningsmetoden...?

1. **... är tidseffektiv, i termer av att riskbedömningen går snabbt att genomföra hos kund?**

inte alls viktigt | lite viktigt | viktigt | ganska viktigt | mycket viktigt | vet ej

2. **... är tidseffektiv, i termer av att du som konsult snabbt kan förstå och ta till dig modellen?**

inte alls viktigt | lite viktigt | viktigt | ganska viktigt | mycket viktigt | vet ej

3. **... tar hänsyn till "mjuka" aspekter av risk (så som rykte och konkurrensfördelar)?**

inte alls viktigt | lite viktigt | viktigt | ganska viktigt | mycket viktigt | vet ej

4. **... genererar detaljrika resultat till kunden (så som utförliga tabeller och grafer)?**

inte alls viktigt | lite viktigt | viktigt | ganska viktigt | mycket viktigt | vet ej

5. **... genererar resultat som är enkla att kommunicera till ledningen?**

inte alls viktigt | lite viktigt | viktigt | ganska viktigt | mycket viktigt | vet ej

6. **... genererar resultat som är enkla att kommunicera till hela verksamheten?**

| inte alls viktigt | lite viktigt | viktigt | ganska viktigt | mycket viktigt | vet ej |
|---|---|---|---|---|---|
| ○ | ○ | ○ | ○ | ○ | ○ |

7. **Har du andra förslag på faktorer som är viktiga för en lyckad riskbedömningsmetod? Ange gärna dessa nedan**

8. **Övriga kommentarer**

Skicka in denna enkät

# Appendix C: Workshop questions

*Syfte med workshopsession II:*

- Att förstå hur workshopdeltagarna tyckte att det var att arbeta MaRiQ under workshopsession I, samt
- Att undersöka hur väl workshopdeltagarna tyckte att modellen uppfyllde de etablerade kraven

*Frågor som ställdes under workshopsession II:*

- Spontant: hur kändes det att arbeta med MaRiQ?
- Hur tyckte ni det var att arbeta med den kvantitativa metodiken jämfört med den kvalitativa?
- Vad skulle behövas för att ni skulle börja använda MaRiQ i ert vardagliga arbete idag?

- Hur tyckte ni att det var att ta till sig och förstå resultaten?
- Hur skulle det kännas att presentera sådana här resultat för organisation och ledning?
- Vad ni tyckte ni om att se *både* den totala och enskilda riskbilden?
- Hur tyckte ni att det var att se *olika* typer av resultat från simuleringarna (top 10 risks, heatmap och uncertainty)?
- Tycker ni att MaRiQ känns praktiskt användbar? Känns modellen tidseffektiv?
- Hur upplevde ni det var att skatta risker i form av intervall?
- Hade ni kunnat tänka er att också uppskatta ett ytterliggare värden, eller var det tillräckligt med den övre och undre gränsen för sannolikhet och konsekvens?
- Upplever ni att modellen hjälper er med att prioritera risker – i så fall på vilket sätt?
- Upplever ni att modellen genererar resultat som känns välgrundade och vetenskapliga?
- Vad tror ni om möjligheterna att använda den här modellen på andra analysobjekt än det vi analyserat här?
- Hur upplevdes tydligheten i modellens 11 steg?
- Hade ni önskat mer detaljerade modellinstruktioner?
- Hur uppfattades balansen mellan simplicitet och komplexitet – i både användandet och resultaten?

# Appendix D: Calibration techniques

***Anti-anchoring:*** Anchoring is a term retrieved from the field of psychology, aiming to describe how people tend to rely too heavily on the first piece of information given to them. Simply thinking of a number before making an assessment will affect the estimate, even if it is a completely unrelated topic (Kahneman, Tversky and Slovic, 1982). Therefore, as an assessor, it is important to try to avoid anchoring. This can be done by thinking of range questions as binary questions, asking yourself: "Am I 95% sure that the true value is over/under the stated lower/upper bound?" (Hubbard and Seiersen, 2016, p.145). Simply being aware of the anchoring effect also help experts improve their estimates (Tetlock, 2015, p.120).

***Combine expert estimates:*** It is proven that the estimates can be improved by letting the experts make estimations separately and then use mathematical methods to obtain a combined estimate. One simple method proven to perform well, is to average the estimates from several experts (Clemen and Winkler, 1999). There are also more complex methods that can be used to combine estimates, such as taking the taking the weighted average of the relative cumulative percentiles (Vose, 2008, p.410-412).

***Equivalent Bet Test:*** It is not entirely easy to know whether one's estimated ranges are actually representing a certain level of confidence. To test whether you really are, let us say, 90% confident in a range, some scholars promote the use of the so called equivalent bet test.

The equivalent bet test is perhaps best illustrated through an example and the one given here is based on the work by Hubbard and Seiersen (Hubbard and Seiersen, 2016, p.139). Let us say that you have estimated a 90 % confidence interval of the monetary impact of the theft of equipment to your business, and you are offered a chance to win 10 000 SEK in one of two ways:

I. You win 10 000 SEK if the true monetary impact lies between the lower and upper bound you stated. If not, you win nothing.

II. You spin a dial divided into two slices, one representing 90 % of the total surface and the other represents 10 % as shown in Figure 1. If the dial lands on the big slice, you win 10 000 SEK, but if it lands on the small one you win nothing.

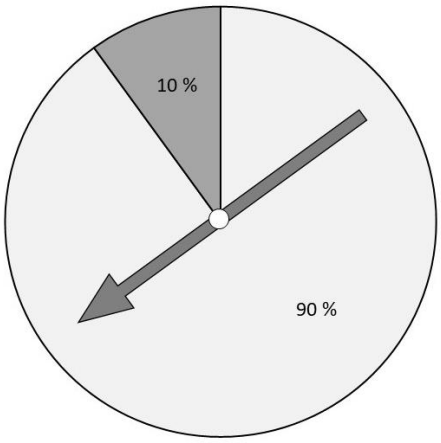



*Figure 1. Spin the dial.*

Which option would you prefer? Truth is that most people (around 80 %) would choose to spin the dial (Hubbard and Seiersen, 2016, p.140). This indicates that most people would think that the dial has a higher chance of paying off, which means that your 90 % confidence interval was not really your 90 % confidence interval. If it were, you would be indifferent to option I and II, since they should actually represent the exact same confidence.

This example clearly points to the function of the equivalent bets. Research have shown that even by just pretending to bet money on a specific estimation, people's ability to assess odds significantly improve. Therefore, comparing your estimations to a bet that you consider equivalent, can help you make more successful forecasts (Hubbard and Seiersen, 2016, p.141).

***Red teaming:*** Red teaming is a form of *alternative analysis*-technique, borrowed from the American military. The red team aims to find alternative arguments to the prevailing view and to seek out other information that do not support the current theory (Mulvaney, 2012). Hence, the purpose of read teaming is to have someone acting as the "devil's advocate", to challenge the assumptions made by the assessor and identify faulty logic or flaws in the analysis (CORE Security, 2019)**.**

# Appendix E: Lognormal distribution computations

The following computations show how we go from an estimated lower bound (LB) and upper bound (UB) of a 90% confidence interval to a lognormal distribution of the variable X. The distribution is found by obtaining the mean and standard deviation of the distribution, which is used to determine the shape of the lognormal curve. The 90% confidence interval means that there is a 5% chance the result end up lower than LB and a 5% chance the result will end up higher UB.

Denotations:
a = ln(LB)
b = ln(UB)

It follows by the definition of lognormal distributions that the natural logarithm of X is normal distributed (Alm and Britton, 2008). This infers that we can write our introduced variables *a* and *b* in probabilities, as shown in Equation 1.

$$\begin{aligned} \mathrm{P}(\ln X < a) &= 0.05 \\ \mathrm{P}(\ln X > b) &= 0.05 \end{aligned} \tag{1}$$

We then introduce the standardised variable Z, which follows the normal distribution with mean 0 and standard deviation 0, Z~N(0,1). The expression for Z is shown in Equation 2.

$$Z = \frac{lnX - \mu}{\sigma}, \qquad Z \sim N(0,1) \tag{2}$$

Where μ is the mean and σ is the standard deviation of the natural logarithm of X. Based on this, we can combine Equation 1 and 2 as shown in Equation 3.

$$P\left(\frac{lnX - \mu}{\sigma} > \frac{b - \mu}{\sigma}\right) = P\left(Z > \frac{b - \mu}{\sigma}\right) = 0.05 \tag{3}$$

Since the standard normal distribution is often used in calculations, there exist a simplifying table with quantiles. The quantiles, denoted with $\lambda_\alpha$, corresponds to values on the x-axis where the area under the curve for values greater than λ is α. This relationship is displayed in Figure 1 and Table 1.

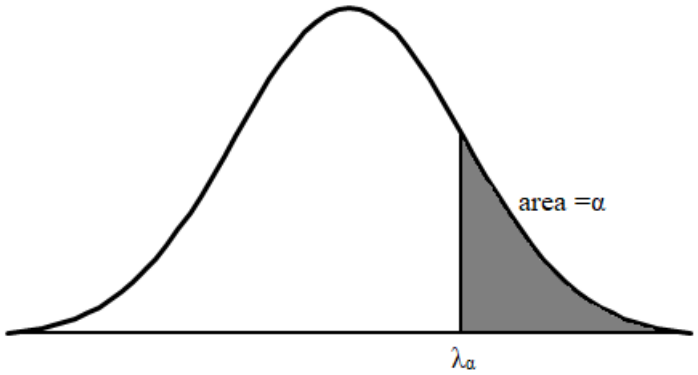



*Figure 1. Normal distribution showing that the area under the curve for values greater than $\lambda_\alpha$ is equal to α.*

*Table 1. Quantiles for the normal distribution*

| α | 0.0005 | 0.001 | 0.005 | 0.01 | 0.025 | 0.05 | 0.10 |
|---|---|---|---|---|---|---|---|
| $\lambda_\alpha$ | 3.29 | 3.09 | 2.58 | 2.33 | 1.96 | 1.64 | 1.28 |

Definition quantile $\lambda_\alpha$:

$$P(X > \lambda_\alpha) = \alpha \; eller \; \Phi(\lambda_\alpha) = 1 - \alpha$$

Based on Table Y and Equation 3, we can write the probability for our introduced standardized variable Z as shown in Equation 4.

$$P(Z > \lambda_{0.05}) = P(Z > 1.64) = 0.05 \tag{4}$$

Comparing Equation 3 and Equation 4, we obtain expressions containing $b$, $\mu$, and $\sigma$ as shown in Equation 5.

$$\frac{b - \mu}{\sigma} = 1.64 \tag{5}$$

Repeating these computations for variable $a$, we obtain the expression shown in Equation 6.

$$\frac{a - \mu}{\sigma} = -1.64 \tag{6}$$

The reason for the minus sign on the right hand side is due to that a is negative in the standardised normal distribution. Equation 5 and 6 forms an equation system that can be rewritten as shown in Equation 7.

$$\begin{cases} a = \mu - 1.64\sigma \\ b = \mu + 1.64\sigma \end{cases} \tag{7}$$

With some algebra, we obtain expressions for $\mu$ and $\sigma$ shown in Equation 7. These expressions are used when modelling the lognormal distribution.

$$\begin{cases} \mu = \dfrac{a+b}{2} = \dfrac{\ln(LB) + \ln(UB)}{2} \\ \sigma = \dfrac{b-a}{3.29} = \dfrac{\ln(UB) - \ln(LB)}{3.29} \end{cases} \tag{8}$$

# Appendix F: Uniform distribution computations

The following computations show how we go from a 90% confidence interval to obtain the maximum and minimum value of the uniform distribution. The maximum and minimum values are required parameters in order to use the uniform distribution in simulations.

We introduce:

u = upper bound of 90% confidence interval
l = lower bound of 90% confidence interval
a = minimum value of distribution
b = maximum value of distribution
h = the height of the distribution

Figure 1 shows the introduced variables *u*, *l*, *a*, and *b* in the uniform probability density function.

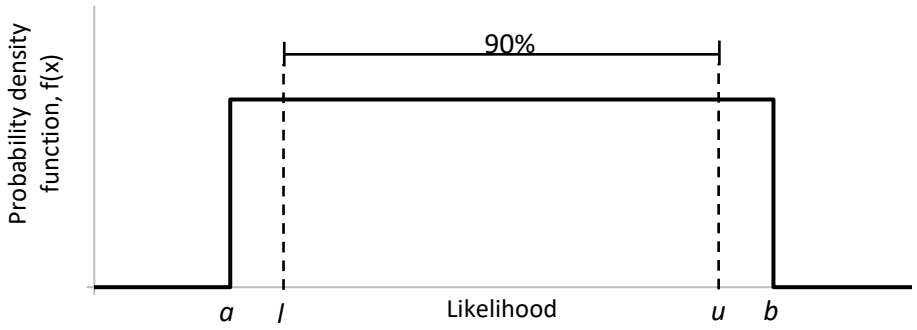



*Figure 1. The probability density function for the uniform distribution with minimum value a and maximum value b.*

The values of *l* and *u* are known from the experts' estimations. We want to compute the values of *a* and *b*. The area under the probability density function always equal 1(Vose, 2008, p.594). Due to the rectangular shape of the distribution, the area is calculated by multiplying the height with the width of the interval. Thus, we can express the height, *h*, of the distribution in terms of *a* and *b*. The expression for *h* is shown in Equation 1.

$$h = \frac{1}{b - a} \tag{1}$$

From the 90% confidence interval, we also know that there is a 5% chance the value will fall lower than *l* and a 5% chance it will be greater than *u*. This corresponds to that the area bounded by *a*, *l*, and *h* equal 0,05. Similarly, the area bounded by *u*, *b*, and *h* does also equal 0,05. The expressions for these areas are expressed in Equation 2 and 3.

$$(l - a) * h = 0.05 \tag{2}$$

$$(b - u) * h = 0.05 \tag{3}$$

Inserting the expression for *h* in Equation 1 into the expressions in Equation 2 and 3 gives an equation system with the two unknown values of *a* and *b*, found in Equation 4 and 5.

$$(l - a) * \frac{1}{b - a} = 0.05 \tag{4}$$

$$(b - u) * \frac{1}{b - a} = 0.05 \tag{5}$$

Finally, we solve the equation system to obtain expressions for *a* and *b* shown in in Equation 6 and 7. These expressions are used when modelling the uniform likelihood distribution.

$$a = \frac{0{,}95l - 0{,}05u}{0{,}9} \tag{6}$$

$$b = \frac{0{,}95u - 0{,}05l}{0{,}9} \tag{7}$$