Linköping University | Department of Computer Science
Master thesis, 30 ECTS | Informationsteknologi
202017 | LIU-IDA/LITH-EX-A--2017/001--SE

Evaluation of quantitative assessment extensions to a qualitative risk analysis method

Utvärdering av kvantitativa bedömningsutvidgningar till en kvalitativ riskanalysmetod

Louise Svensson

Supervisor : Marcus Bendtsen
Examiner : Nahid Shahmehri

LINKÖPING UNIVERSITY

Linköpings universitet
SE–581 83 Linköping
+46 13 28 10 00 , www.liu.se

Abstract

The usage of information systems (IS) within organizations has become crucial. Information is one of the most vulnerable resources within an enterprise. Information can be exposed, tampered or made non-accessible, where the integrity, confidentiality or availability becomes affected. The ability to manage risks is therefore a central issue in enterprises today. In order to manage risks, the risks need to be identified and further evaluated. All kind of threats with the possibility to negatively affect the confidentiality, integrity, or availability of the organization need to be reviewed. The process of identifying and estimating risks and possible measures is called risk analysis. There are two main categories of risk analysis, qualitative and quantitative. A quantitative method involves interpreting numbers from data and is based on objective inputs. A qualitative method involves interpreting of subjective inputs such as brainstorming and interviews. A common approach is to apply a qualitative method, however a lot of criticism has been raised against using subjective inputs to assessing risks.

Secure State is a consulting company with specialist expertise in the field of information security. They help their customers to build trust in the customers systems and processes, making their customers businesses operate with consideration to information security. One service offered by Secure State is risk analysis, and currently they performs qualitative risk analysis. Given all criticisms against a qualitative approach for assessing risks, this study developed a quantitative risk analysis method for Secure State. According to participants, who attended at a risk analysis where the developed quantitative risk analysis method was used, the quantitative risk analysis method improved the risk assessment. Since risks and their effects are decomposed into smaller components in the proposed quantitative risk analysis method, interpretations of risks and their meaning during assessments less likely differed. Therefore, the common understanding of a risk increases, which makes the quality of the evaluation of risks increase. Furthermore, the usage of statistical data increases in the developed quantitative risk analysis method. Additionally, the quantitative method handles the fact that all data used is imperfect. The data is imperfect since it is used to describe the future, and the future has not happened yet.

Acknowledgments

This study was conducted together with a smaller consultancy firm, Secure State, operating within IT security. Firstly, the author wants to acknowledge the supervisor at Secure State, Jan Karlsson, giving his effort by supporting the author with guidance, knowledge and the ability to contact different stakeholders, in order to gather the required information. Furthermore, the employees at Secure State has shown a great commitment during the course of the study. The employees have been collaborative and the they have shown a great interest in the author's work. Secondly, the author of the report also wishes to thank the supervisor of the study at Linköping University, Marcus Bendtsen. Marcus Bendtsen has been a great support during the course of the study, and provided guidance making the study proceed in the right direction. Finally, the author wishes to thank the students' opponent, who have come up with rewarding feedback during the course of the study.

Linköping, June 2017
Louise Svensson

Contents

List of Figures

List of Tables

1 Introduction

The ability to manage risks is a central issue in enterprises today [6]. Information is one of the most vulnerable resource within an enterprise. Information can be exposed, tampered, or made non-accessible, which negatively affects the integrity, confidentiality, or availability (CIA). Therefore, information must be protected and managed in a secure way. In order to protect the information and obtain a secure information management, the importance of the provided information and threats toward the information must be identified and managed [37]. The usage of information systems (IS) within organizations has become crucial, however risks associated with the system needs to be managed. The risks are not only limited to the system itself, such as the hardware and software, but organizational adoption, legislation, and how users manage information are also critical components important to consider in the process of risk management. All kind of threats with the possibility to negatively affect the confidentiality, integrity, or availability of the organization must be reviewed. Further, evaluation of the threats, based on their probability to occur and following consequences, is necessary and used as a basis for the decision whether a risk needs to be mitigated or not. [26].

In basic terms, a risk analysis constitutes of identifying risks and its accompanying consequences. The internal standard organizations (ISO) divides risks into two main components [26]:

- Vulnerability, such as a weakness in a system, procedure, design, entity, or implementation.
- A threat, which is a potential cause of an incident that may harm a system and further the organization.

There are different methods for performing risk analysis. The risk analysis methods are divided into three main categories: quantitative, qualitative, or a combination of quantitative and qualitative. A quantitative method involves interpreting numbers from data and is based on objective inputs. A qualitative method involves interpreting of subjective inputs, such as brainstorming and interviews. A combination of the two risk analysis approaches, called a hybrid method, consists of both objective and subjective estimations. These three categories of risk analysis will be further described in Section 2.3. Regardless of the method used for performing risk analysis, the aim of performing risk analysis is to identify and mitigate risks

that may have a negative impact on an organization and are evaluated to harm the organization's business in the future [13]. In order to consider a risk analysis useful, the method must generate results of good quality, i.e. be defensible. In order to provide results of good quality the process of creating the results shall be based on available information and be structured thoroughly i.e. be developed by using . Furthermore, the risk analysis method needs to be productive and efficient.

The process of conducting risk analysis requires the organization to spend resources, such as time, competence, and money. Depending on the risk analysis method used the efficiency of the process varies. The efficiency of the process can varies in terms of comprehension of the assessment, quality of the results, and required resources. The choice of risk analysis method is therefore a key-decision with the potential of increasing the usefulness of a risk analysis method. [26].

A common approach today is to apply a qualitative method for performing risk analysis, however a lot of criticism has been raised against using only subjective inputs to assessing risks [13]. For example the criticism indicates that by only using subjective inputs to identify and estimate risks, errors are introduced, and the outcome dose not apply to the reality of the situation [13].

1.1 Aim

Secure State is a consulting company with expertise in the field of information security. They provide services to their customers, making the customers build trust in their systems and processes. One service offered by Secure State is risk analysis. Currently the risk analysis performed by Secure State has a qualitative approach. Given all criticisms against a qualitative approach for assessing risks, this study intends to develop a quantitative risk analysis method for Secure State to apply when performing risk analysis. Developing a quantitative risk analysis aims to improve the results of the risk analysis in terms of precision and accuracy.

1.2 Research questions

1. Which pros and cons exists in the current risk analyses methodology performed by Secure State?
2. How can the result be improved by including quantitative measurements during a risk analysis. How should a quantitative approach be used when performing risk analysis at Secure State?
3. How can different key components from both qualitative and quantitative risk analysis methods be combined in order to make Secure State extract improved results from their risk analysis?

The initial approach will consist of analyzing, evaluating and comparing available quantitative methods for conducting risk analysis. One key component that needs to be addressed is why quantitative risk analysis can be considered useful and appropriate. The process of gathering knowledge regarding performance of quantitative risk analysis shall be based on a review of scientific theory in the field of performing risk assessments through quantitative risk analysis. Furthermore, the theory review aims to identify important components in order to gain successful results from quantitative risk analysis methods. Secure State wishes to offer a method based on a quantitative approach as a complement to their current qualitative approach. Therefore this study further will examine the pros of adding a quantitative method, or include quantitative components in their existing qualitative risk analysis

method. In order to improve Secure State's current risk analysis method an evaluation of their current risk analysis method will be performed. This evaluation aims to identify pros and cons within Secure State's approach. Observations will be conducted during risk analysis, interviews will be performed where employees at Secure State will be the respondents, and document reviews from earlier performed risk analysis will be conducted. Performing the observations, interviews, and document reviews enables comprehensive gathering of data regarding how Secure State performs risk analysis and their accompanying problems.

A quantitative risk analysis method will be proposed in order to answer the second research question. The risk analysis methodology selected should have a quantitative approach, and meet requirements from ISO 27005. To identify components to add into Secure State's current process of performing risk analysis, the focus will not be limited to risk analysis specific to information security. To evaluate the result of the selected quantitative risk analysis method proposed for Secure State, a qualitative approach for evaluation will be applied. A risk analysis will be performed where the proposed quantitative risk analysis method will be applied. Participants during this risk analysis shall answer a predefined questionnaire based on a modification of the System Usability Scale, (SUS). The questionnaire will gather information regarding participant's thoughts on the performance of the proposed quantitative risk analysis method, as well as on the outcome of the risk analysis.

1.3 Delimitations

Secure State is today performing a qualitative approach for conducting risk analysis at their clients, including both risk identification and risk assessment. The approach of the risk analysis, which Secure State performs, has been developed to be appropriate for different clients operating in different types of industries, and having different requirements regarding the acceptable amount of resources spent on a risk analysis, such as time and money. The current risk analysis performed by Secure State requires the client to contribute with participants having the knowledge needed for the specific risk analysis and prepare the scope of the analysis. If the clients cannot provide sufficient participants for the risk analysis, the analysis will become incomplete and therefore decreasing the quality of the results. Leading the risk analysis, compiling and analyzing the result of the risk analysis, and further present action proposals in order to mitigate the risks in need are responsibilities of Secure State. The action proposals presented by Secure State is based on the result from the risk analysis. In order to reuse the parts considered appropriate of Secure State's current risk analysis method, this study focuses on identifying and evaluating risk analysis of a more quantitative form, yet adaptable to how Secure State performs risk analysis today. Hence, the selected quantitative risk analysis shall be able to be performed in workshops. Furthermore the selected quantitative method shall both identify and estimate risks and measures, and provide clients with decision support. The aim is to create a hybrid version of Secure State's way of performing risk analysis today. A hybrid version includes both qualitative and quantitative processes within the risk analysis method [21]. Methods and approaches considered not suitable or appropriate to use as a combination with Secure States way of work today will therefore not be evaluated further. Additionally, Secure State has stated some initial requirements which the risk analysis method selected needs to fulfill, these requirements are:

- The methods shall including a quantitative approach.
- The methods shall be applicable without the need of purchasing support for measuring the risks.
- The methods shall meet requirements of ISO 27005.

2 Theory

In this chapter, Section 2.1 will describe general components of risk analysis and Section 2.2 presents general challenges regarding risk analysis and their performance. In Section 2.3 a description regarding differences between different types of risk analysis methods will be presented, both in terms of their approaches and gained results. Section 2.4 provides information regarding the ISO 27005 standard, an overview of what the standard is and stands for, and why the standard should be considered during risk analysis will be discussed. Finally, Section 2.5, 2.8, 2.6, and 2.7 describe the quantitative risk analysis method, the risk estimation method, the distribution algorithm, and the probability distribution method, which the selected and modified quantitative risk analysis method presented for Secure State (see Section 4.3) is based on.

2.1 General knowledge of risk analysis

In order to protect something, it is necessary to identify what it is and what it needs to be protected from. Conducting risk analysis allows an organization to "know themselves" with respect to their risk exposure [19]. Risk analysis intend to identify and evaluate risks in sense of their impact on the business and further initiate a plan for mitigate risks considered necessary to be mitigated. The result of an risk analysis presents an interpretation of what to expect in the future for an organization. [9].

The motivation for performing risk analysis

Comprehensive risk assessment of potential risks and further risk management, is a fundamental decision-making process where the organization must consider different types of threats. Some examples of different types of threats are [9]:

- Malicious actions
- Human error
- Mechanical failure
- Process failure

- Natural (e.g. weather, geological activity)
- Cyber risks

The purpose of performing risk analysis is to identify threats and further assess the impact of the threats toward the business, to see whether the risks must be mitigated or can be considered acceptable. Conducting risk analysis can be seen as a quantification of uncertainty. Risk analysis is primarily an exercise of measurements, essential for identifying and measuring risks and the level of accompanying exposure [26]. In basic terms, the risk is measured by the probability of an event to occur and its consequences. Consequences for an organization's business can consist of different types of losses. Consequences of a threat can both affect tangible and intangible assets. A tangible asset is an asset having a physical form. Tangible assets includes both fixed assets, such as machinery, buildings, and land and current assets, for example inventory. Intangible assets are the opposite of tangible assets, and are described as nonphysical assets. Examples of intangible assets are reputation, trademarks, copyrights, goodwill and brand recognition [15]. Estimation of the consequence of a tangible asset is in many occasions an easier task than estimating the consequence of intangible assets. For instance, it is difficult to predict the loss of reputation and how that loss further will affect the organization. Calculating accompanying losses of a non-functioning machine and the cost of replacing it for an organization is more intuitive [13]. Despite this, measuring the consequences is often seen as an easier task than evaluating the probability of a threat to occur. That is explained by the fact that it is a difficult task to predict the future in terms of what to expect [13, 26].

To gain valuable results from a risk analysis, the scope shall be clearly defined, and participants must possess proper knowledge. Include participants from different departments enables to identify risks and threats from different angles, giving the assessment a higher rate of completeness [13]. Additionally, it is important that participants, within the risk analysis, have positions high enough in the hierarchy of the organization to be able to make decisions related to the assessment, without the need of passing it further for approval. A beneficial size of the group depends on the organization as well as the scope of the risk analysis. A big organization, where the risk assessment regards a broad area requires more people compared to a little organization examine a small scope. The complexity of the assessment and the data collection is another aspect affecting the appropriate size of the assessment group. Time limits and deadlines are also indicators regarding the quantity of participants appropriate.

To properly conduct a comprehensive risk analysis it is also important to consider correlations among risks. Correlations among risks have high significant on the result of the risk analysis and requires to be included in the risk assessment in order to provide realistic results [13]. The correlations among risks can be described as a chain of risks where a realization of the first risk within the chain would affect either the probability or the consequence of the second risk within the chain. If the first risk realizes, the second risk's probability or consequence could either increase or decrease, making the correlation among the risks be both positive or negative for an organization.

Furthermore, it is useful to troubleshoot the result, i.e. when the result is gathered, troubleshooting it in order to increase the credibility. Does the result make sense, or does it includes some form of misleading parts, etc. [9].
Risk analysis is an approximation of reality, based on imperfect data. The reality is far to complex to be modelling exactly, and the future will always stay uncertain. Decomposing a complex subject into a clearer and easily analyzed component, allows us to understand and make reasoned judgments. Therefore, decomposing risks during the process of estimating risks improves the outcomes from a risk analysis. To further optimize the use of imperfect data, inherently designed methods can be applied to deal with uncertainty in data [13].

Components of risks

There are multiple definitions of risks depending on the information security standard applied. An information security standard is a framework for IT security assurance [9]. The fundamental definition according to a lot of information security standards is that a risk is the product of the probability of a threat to occur towards the organization and its accompanying consequences on the organization, see Equation 2.1 [33].

$$Risk = Probability * Consequence \tag{2.1}$$

To further understand the meaning of probability and consequence, this report views risks according to a definition presented by the National Institute of Standards and Technology (NIST) and Factor Analysis of Information Risk (FAIR) institute. NIST and FAIR define a risk as "*the probable frequency of loss events and probable magnitude of future loss*", see Figure 2.1. The frequency of a loss event can be described as the frequency, within a given time-frame, that the loss event will occur. A loss event is a threat event that has resulted in loss for the organization, where a loss can be described as a negative consequence on an organization's resources or assets. Furthermore, a threat event can be described as a threat actor (i.e. a person or the nature) who acts in a manner that has the potential to cause loss for the organization.

Loss magnitude is the total loss for the organization when a loss event occurs. Different forms of loss can arise from a loss event, e.g. loss of the organization's reputation or loss of the organization's productivity. Commonly, the loss affects the organization's business in a negative way [9].

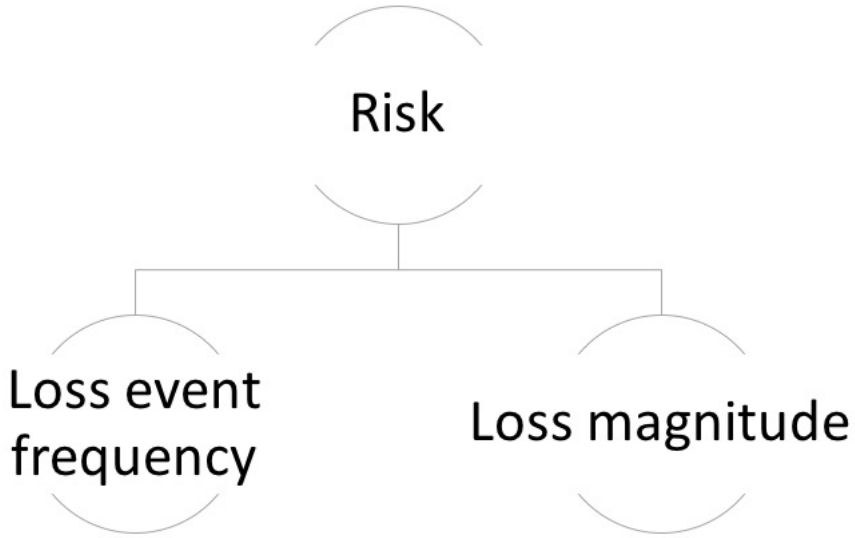

Figure 2.1: *Components of a risk according to FAIR.*

The wording within the definition of a risk, according to NIST and FAIR, i.e. using the words probable frequency and probable magnitude is often considered complex. However, the wording is important for a few reasons [9]:

- A risk analysis should include the two components frequency of a loss event and its loss magnitude in order to be meaningful. Knowing the loss of a threat event if the frequency is not analyzed is relatively meaningless. Likewise, knowing the frequency of a threat event is relatively meaningless without understanding the threat event's loss magnitude.
- Risk analysis is based on imperfect data and models. By imperfect data and models means an approximation of what is expected based on statistics from similar known risks and parameters (such as outdated systems or firewalls) that might increase or decrease the probability of a risk to occur or the consequence if a risk has occurred. The usage of imperfect data and models for estimating risks requires to consider any statement of loss events frequency or loss magnitude as a probability.
- The probability of a threat must be described within a given time-frame in order to be meaningful, i.e. be described as a frequency.

The terminologies within the definition of risk used by FAIR can often appear to be overwhelming and difficult to understand [33]. However, when the terminologies are understood they become useful during risk analysis. As an example, the word probability is commonly used within risk analysis. FAIR describes probability as a frequency, making the probability be estimated within a given time-frame. Using the frequency makes it easier to have a common understanding towards the meaning of a certain value for the probability, and therefore increase the credibility of the determined significance of mitigating the risk [9].

2.2 Challenges in risk analysis

Estimating the future, i.e. the unknown, is a central task during a risk analysis, however a challenging task to perform [13]. Since the estimation regards the future, there is no information available which ensures providing a correct answer. The possibility of making a good estimation however increases by using a risk analysis method which utilizes the available resources in an appropriate way [3, 12]. For example, available resources can include information regarding statistics of similar risks, information regarding currently security mechanisms implemented, or the size of the potential threat actors etc. How to utilize the available resources in an appropriate way varies dependent on risk analysis method used. For instance, the FAIR ontology divides a risk into small components making it easier to identify and utilize available information in a correct manner [9].

Critic towards qualitative risk analysis methods

Some experts in risk management argue that applying a qualitative method for risk analysis, and only rely on subjective inputs, is equal as not having risk management at all [12]. Qualitative methods, referred to as soft methods, are mostly experience based, and by several risk managing experts not considered validated. By the usage of subjective inputs for identifying and scoring risks, error are introduced, and the outcome does not apply to the reality of the situation. Humans do mistakes, and during risk analysis participants seem to repeat consistent types of errors in the process of identifying and judging risks [13]. Research has revealed that there are quantitative processes with the potential of correcting the systematic errors commonly occurring in human decisions [12]. Quantitative approaches for risk analysis often include historical data and real-world observations. Decisions, only based on subjective inputs, are unreliable due to the following factors [13]:

- Experience represents non-random and non-scientific samples of events throughout a persons lifetime.
- Experiences are based on memories, which humans are very selective regarding what to remember.
- What humans commit to memory may contain several logical errors.
- Reliable feedback to previous decisions are necessary in order to trust experiences.
- Regardless of the amount of accumulated experiences, the application of the experiences will still contain inconsistency.

What humans recall and further interpret is related to the concept called bias. Bias is a tendency to think and behave in a way that interferes with rationality and impartiality. The absence of objective inputs in the complex process of estimating risks cause decisions to rely on bias in a greater extent [13]. As mentioned, only a fraction of impressions and events becomes memories. One factor that has a big impact on the, in many occasions, unconscious choice of what to remember is called the *peak and rule*. It means that the tendency is to remember extremes of experience not the mundane [11]. The tendency of remembering the extremes will have an impact on the assessment of risks, were logical errors within the assessment will occur [13]. Additionally, a factor affecting the result of a risk analysis is based on a phenomena discovered by Judgement and Decision-Making psychologists, saying that people generally are naturally overconfident in their predictions [32].

2.3 Quantitative vs Qualitative risk analysis

Risk analysis methods should be evaluated based on the following criteria [9]:

- Is it useful?
- Is it practical?
- Are the results defensible?

In order for the results of a risk analysis to be useful and defensible, they requires to meet a proper level of accuracy, still having the best possible precision. During this thesis, accuracy refers to obtaining values where the correct value is covered. Precision is the possibility of estimate values witch are close approximated to each other. This means that the estimated range of a risk's possibility to occur (for instance) shall include the probable correct value in order to gain accuracy. If the possible information regarding the risk's possibility to occur is inadequate, it makes it harder to be precise in the estimated range in order to still verify the accuracy. Then, the range of possible values for the risk's possibility to occur requires to be extended. While the range is extended the level of obtained precision within the estimation is decreased. It is important to always try to achieve maximum precision based on the current information available regarding a risk, yet not loose the accuracy.

Qualitative risk analysis method

Scoring risks is a common approach for risk evaluation using a qualitative risk analysis method. The risk analysis method and how the risks are scored can differ, but the outcome is presented in a relative order. A numeral scale as 1 to 5, or ratings by "high/medium/low" are scales common used in qualitative risk analysis methods. There are two main categories of qualitative risk analysis methods [13]:

- The additive, using *weighted scores*.
- The multiplicative, using *risk matrices*.

Weighted scores include several ordinal scores, where the score for a risk's probability and consequence are added into a joined score to present the importance of mitigating the risk. Risks matrix uses either two ordinal scales, *likelihood and impact* or three, *threat, vulnerability, and consequence*. These (either two or three) scales are multiplied into a final risk value. The matrix approach is popular and commonly used when performing risk analysis and has been given much attention from various international standards organizations [13]. National Institution of Standards & Technology (NIST) represents one standard of a matrix based risk assessment, using *high, medium, and low* to estimate risks. The likelihood and impact are rated through this three-graded scale (high, medium, low) separately. The result of the two rated factors for a risk, i.e. the likelihood and impact, are presented in a matrix, where some combination of the likelihood and the impact are accepted and others not, to see whether a risk is considered in need of mitigation or considered acceptable by the organization. The ranking scale is pre-defined, where each level of the scale is linked to a definition and description of its meaning [14].

Applying a method from one of these two groups, i.e. additive or multiplicative, referred to as scoring methods, has three main problems [12]:

- The methods are usually developed in isolation from researches.
- They do not consider the issue regarding perception of risks and uncertainties.
- The qualitative descriptions of likelihood and consequence are understood and used very differently by different people, even though deliberate steps are taken to defining the meaning of the grades.

These issues make the results of a performed qualitative risk analysis arbitrary, and lacking of credibility. Furthermore, evaluating a risk's estimated likelihood and impact as ordinary scales, i.e. adding or multiply the likelihood and impact values, are not appropriate and might lead to unintended consequences [13]. The scales are not appropriate to multiply since the impact and the likelihood do not represents the same thing, and the result will therefore not respond to reality. An example will be described in order to increase the understanding regarding why it is not appropriate to multiply the impact value and the likelihood value into a common risk value. If one person is rating a certain movie with five stars, and five persons are rating another movie with one star each, the result of multiplying the number of stars with the number of persons would be a value of five for both of the scenarios. The result would therefore not respond to the reality since the common value five represents different things and can not be compared between the two scenarios [13]
.
A risk analysis method can be considered useful when the results are accurate and meaningful to the decision-makers. Results expressed in qualitative or ordinal scales need to be questioned based on its meaningfulness. The outcome from a risk assessment based on a qualitative process, where the risk analysis results in a risk score, is necessarily not logical in sense of what the risk value represents, see Section. A lower risk score is intuitively better than a higher, but what exactly dose a risk value represents where a "high" consequence has been multiplied with a "small" likelihood. As of accuracy, a precise ordinal rating implies a level of precision that is unrealistic in risk analysis. The accuracy is often a matter of what assumptions were being made and how rigorous the thinking that underlies the analysis was [13].

Qualitative scoring is a mental model based on persons thoughts of what a risk implies, and biases might emerge making the odds lower that persons mental models will be as good as a well-vetted formal model. Likewise, qualitative scoring uses imperfect data to justify ratings which assumable has been collected and developed with much less rigor, implicate that the result of a well-developed quantitative approach will be more accurate and reliable than a qualitative approach [9].

Quantitative risk analysis methods

Regardless of applied risk analysis method, the main stages within risk analysis is to identify risks, determine its impact, and establish action plans to avoid harm for the organization. The fundamental decision support is based on risk values, consisting of the probability of a risk to occur and its consequences. In quantitative risk analysis methods probability and impact are represented as monetary values, and based on statistics and historical data [13]. To properly base risk assessments on statistics, large samples accessed during a proper period of time are required. In order to addressing risks that appears rarely, a good time frame is required. Base risk assessments on statistics however makes the risk analysis require more resources, for example time, making the risk analysis less practical [13]. On the other hand, one can question why quantitative risk analysis even are legitimate due to the imperfection of the models and the data.

Important to consider in risk assessments is the difference between possibility, probability, and frequency. Possibility and probability is two separate factors, but commonly used in confusion during risk assessments. A possibility is an estimation of "yes or no", for example "Is it possible for a cyber attack to occur?", while a probability refers to the extent to which a threat is likely to happen [13]. Frequency can be described on a time line basis and generally used in quantitative approaches for performing risk analysis. Using frequency is said to be beneficial in order to create a common understanding towards the mean of probability. Ar-

guments raised about quantitative risk analysis is based on the impossibility of knowing the exact probability or consequence, and some argue that it needs to be treated as possibilities. Furthermore, critics are raised toward the absent of statistical data in many occasions [13]. Available information and data might suffer where only a few measurements are available. The paucity of empirical data often makes quantitative statistical analysis absent.

The foundation of an effective information security risk assessment is data. Without data to support an assessment the performance will lack of credibility. Data collection is the most rigorous and most encompassing activity in an information security risk assessment. Success within the process of accessing data constitutes of several things, where the most basic one is planning. Due to the fact that all subsequent phases of a risk assessment is relying on the quality of accessed data, the collection of data needs to be processed well. In order to gather the data, communication within the organization is essential as well as having participants with the knowledge required for the specific risk analysis. Providing too much or too little information may impair the ability to effectively interact with the individuals that the data assessment is relied on.

During a quantitative risk analysis a sensitivity analysis is advantageously to perform in order to verify the results from historical data and consider the uncertainty within the result. The aim is to identify how sensitive the risk is with respect to changes in input parameters of the risk model. To further determining needed risk-reducing measure, criteria regarding risk acceptance, i.e. an unacceptable level of risk for the organization must be taken into consideration [3].

Combining qualitative and quantitative methods decrease the risk of using unreliable data and increases the opportunities to identify risks and its exposure to the organization, hence a hybrid risk analysis method is a good approach for performing risk analysis [8].

2.4 ISO 27000

ISO 27000 is the root for a whole series of international standards for the management of information security. Developed by a joint committee of the International Organization for Standardization (ISO) in Geneva and the International Electronically Commission, these standards now provide a globally recognized framework for good information security management [5].

Continuously following the framework of the ISO standards provides the organization with an certificate. An accredited certificate tells existing and potential customers that the organization has defined and put in place effective information security processes, this helps in creating a trusting relationship. A certification process also helps the organization focus on continuously improving its information security processes. Of course, above all, certification, and the regular external review on which ongoing certification depends, ensures that the organization keeps its information security system updated, and therefore that it continues to ensure its ability to operate [5]. Figure 2.2 represents the structure of the ISO 27000 series. As mentioned, the 27000 standard represents the root of all standards within the series. The standards, from the ISO 27000 series, discussed during this thesis are highlighted with an orange colour in Figure 2.2 and further briefly described in the following subsections.

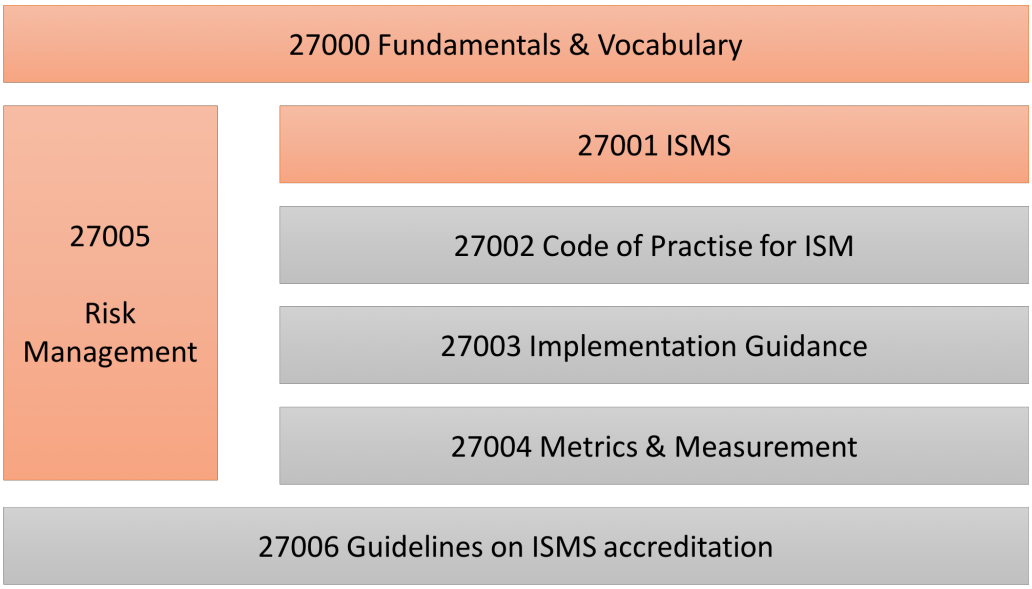

Figure 2.2: *The structure of the ISO 27000 series.*

ISO 27001

A lot of various security standards are available for conducting risk assessments. A security standard is a security framework for establishing an effective information security management system (ISMS). ISO 27001 is a popular, internationally-recognized standard of good practice for information security. ISO 27001 provides the specification for an ISMS. However, an information security standard is not a law, it is a way for a business to attest to another business that they are sufficiently exercising an acceptable level of security controls, important in internationalization among businesses today. The framework of ISO 27001 is considered a top down and risk-based approach [18, 31]. A top down approach for performing risk analysis begins at a high level in the organization. The process of having the risk management initializes at the top-level of the organization makes the risk management specific to the business objectives and focusing on possible threats to the specific organization's achievement. Figure 2.3 presents a view of a top down framework [18]. The top down approach presented in Figure 2.3 initializes risk management in a high risk process. The high risk process refers to risk management in the board of direction within an enterprise. The board of direction analyzes risks by aggregating the impact of internal operational failures. The next step in an top down approach is the moderate risk process, which refers to executive management. Executive management aims to control the implementation of risk management accordingly to the general strategy determined during the high risk process level. The implementation refers to the low risk processes where process owners control the work.

Figure 2.3: *A top down risk based approach.*

Most information systems are not designed from the outset to be secure. Technical security measures are limited in their ability to protect an information system. Management systems and procedural controls are essential components for any information system in order to be considered secure [5]. The first step of creating effective management systems and procedural controls for any information system, and one of the first requirements for ISO 27001 compliance, is to define the risk assessment approach for the organization. According to the ISO 27001 framework, the risk assessment methodology shall be based on the business, the legal and regulatory requirements, and information security. Additionally, the risk assessment methodology should have a criterion for accepting and identifying acceptable risk levels. The framework also highlights the importance of the results gathered through the risk assessment method. The risk assessment needs to be able to reproduce comparable and reproducible results in order to be meaningful for the organization [33].

According to ISO 27001, organizations are able to identify risks by identifying the assets of the organization, threats towards the organization, and vulnerabilities within the organization which impacts the confidentiality, integrity, and availability of the asset. Additionally, the framework of ISO 27001 also requires the organization to further analyze and evaluate the risks identified in sense of the risk's probability to occur and its accompanying consequences towards the organization [33].

ISO 27005

ISO 27005 is the Information Technology-Security Techniques-Information Security Risk Management standard released by the international standards body ISO with the aim of providing practitioners with a guidance over information security management processes that are needed for the implementation of a valuable and effective risk management system. An important part of ISO 27005 is risk assessments, e.g. risk analysis. The ISO 27005 consists of six main topic areas [33]:

- Context Establishment.
- Information Security Risk Assessment.

- Information Security Risk Treatment.
- Information Security Risk Acceptance.
- Information Security Risk Communication.
- Information Security Risk Monitoring and Review.

For this thesis the focus regards the second topic area of the ISO 27005 standard, namely Information Security Risk Assessment. ISO 27005 defines three sequential steps essential during risk assessments [33]:

- Risk Identification
- Risk Estimation
- Risk Evaluation

Risk identification

Risk identification consists of five activities. Firstly, identification of assets, which aims to identify all assets within the scope of the risk assessment. ISO 27005 divides assets into two categories: primary assets and secondary assets. Primary assets are by ISO 27005 defined as the core processes, activities, or information for the organization. Secondary assets are by ISO 27005 considered to be hardware, software, network, personnel, site, and structure [33].

Secondly, identification of threats. The objective is to prepare a list of potential threats for the assets stated during the identification of assets.

Thirdly, identification of existing controls. The objective is to identify the existing security controls within the organization.

Fourthly, identification of vulnerabilities, i.e. identify vulnerabilities which exists for the assets.

Lastly, identification of consequences, hence determining the possible damage or consequence caused if a threat action succeeding to impact the asset in a negative way.

Risk Estimation

During the "Risk Estimation" there are three main activities: assessment of consequences, assessment of incident likelihood, and level of risk estimation [33].

Assessment of consequences means assessing the impact on the organization caused by the threat event. There are different types of impact that can be the result from a threat event, ISO 27005 gives examples such as:

- Investigation and repair time.
- Work time lost.
- Opportunity lost.
- Health and safety.
- Financial costs of specific skills to repair the damage.
- Image reputation and goodwill.

Assessment of incident likelihood is the activity where the likelihood of an incident where a threat has materialized and resulted in a loss is estimated. During this part both qualitative and quantitative techniques can be used and ISO 27005 recommends a combination of the two techniques were the following factors shall be taken into consideration:

- Frequency of occurrence of the threat (statistics).
- Motivation and capability of the source.
- Geographical factors and the environment.
- Vulnerabilities.
- Existing Controls.

The last step during the risk estimation is to decide the level of risk estimation, where the objective is to provide values of the likelihood and consequence, which will ultimately result in a risk value. The risk value can however be represented in different ways depending on the risk analysis method applied. The value can for example be a product of two ordinal scales, commonly used in qualitative risk analysis (see Section 2.3) [13, 33].

Risk Evaluation

Once the risk estimates have been determined, the final activity within the risk assessment steps of ISO 27005 is to prioritize the risks identified. The prioritization of risks shall be based on the risk estimation performed as well as of the risk acceptance specific for the examined organization [33]. This means that a risk which has being estimated with a high probability to occur or a high accompanying consequence, based on the organization's criteria for risk acceptance, shall have a high prioritization. The prioritization of risks aims to provide a guidance of what risks the organization is most vulnerable towards. Risks estimated to have a high priority need to be managed first by the organization [5].

2.5 Quantitative risk analysis methods examined

Each method identified during the literature study was evaluated based on the criteria mentioned in Section 3.3. The methods identified will shortly be described.

The Risk FAIR Ontology

This section is based on information extracted from the book "*Measuring and managing information risk - a FAIR approach*" [9]. The FAIR Book provides a practical and credible model for understanding, measuring and analyzing information risk of any size and complexity within any organization [9].

FAIR's ontology represents a model of how a risk works by describing the factors that make up the risks and their relationships to one and another. Additionally, these relationships are described mathematically, which allows the organization to calculate risks significance. As a result of describing a risk's factors and further calculate the risks, the approach of FAIR's ontology estimates the risks with consistency, in logical terms, and with clear definitions. FAIR's ontology can therefore significantly improve the quality of risk-related communication within an organization.

Scope tables for risk IDs

The first step in the methodology means to identify all possible risks within the scope of the risk analysis. Each identified risk during the initial step of the risk analysis shall be managed individually, hence the rest of the method shall be performed several times depending on the number of identified risks. The aim is to create a "scope-table" for each risk, see Table 2.1. These "scope-tables" intend to divide each risk into four different components:

- Asset at risk.
- Threat Community.
- Threat type.
- Effect.

Each risk might, for example, affecting several assets, based on different threat types, having different effects. Each combination, connected to one risk, of the components (i.e. asset at risk, threat community, threat type, and effect) is called a risk scenario, hence each risk may consists of several risk scenarios. To decide whether a risk needs to be divided into several scenarios a rough estimation is performed. The estimation aims to determine whether the probability or the consequence of the scenarios are likely to be different. If so, they shall be divided into several scenarios and be managed separately. All significant scenarios need to be evaluated in order to estimate the affection of the risk properly.

Table 2.1: *An example of a created scope table*

Asset at risk	**Threat Community**	**Threat type**	**Effect**
Customer information	Privileged insiders	Malicious	Confidentiality
Customer information	Privileged insiders	Accidental	Confidentiality
Customer information	Non-privileged insiders	Malicious	Confidentiality
Customer information	Cyber criminals	Malicious	Confidentiality

Asset(s) at risk

What constitutes the assets at risk? In many cases several assets, important for the organization, are involved. In order to gain maximum value from the risk analysis it is necessary to identify the "real assets". Assets considered as the "real assets" depend on the organization and the scope of the risk analysis. To differentiate assets relevance and its role in an analysis, "container" constitutes a useful term. The "container" is the assets first reached from an attack, however not the goal, i.e. not the assets valuable for the organization. For example, an exposed password can pose a threat to the organization. The password itself is probably not the asset of value, i.e. the password is seen as the container, instead the significant assets are the assets the exposed password leads to, e.g. valuable information or processes.

Threat communities, TComp

Who or what constitutes the threat? Is it humans, animals, the nature, or mechanical? The threat communities can for example constitute of non-privileged insiders and privileged insiders. It is not always necessary to split these into two different threat communities (TComp), some times they can represent one TComp, hence seen as insiders. What determines the need of splitting threat communities are:

- Would threat event frequency be similar across different threat communities?
- Is the threat capability likely to be the same across these threat communities?

- Have the different threat communities the same expectations of reaching the target?

If the response towards these three questions are "yes", it is often preferable adding the TComp into one TComp. Each TComp creates a new scenario which demands creating a separate risk analysis, hence is time consuming. Worth considering during the risk analysis is that estimations in similar scenarios, yet not merged due to inequality in one or several of the three questions presented above, can be reused. Reusing information gathered in an other risk scenario makes the risk analysis less time consuming. The list below gives three example of different TComps:

- Privileged insiders.
- Non-privileged insiders.
- Cyber criminals.

Threat type

Why is the threat occurring? Is the threat malicious, human error, mechanical, process failure or natural? Depending on the type of event, significant differences in the frequency, capability and possibility of reaching the target, often occur. If the threat type can be seen as similar for the selected type of TComp, no further division is required.

Effect

Finally it is necessary to understand and identify how the threat scenarios affect the asset. For information security scenarios, the effect on the asset can be identified as loss of confidentiality, integrity, or availability. Most scenarios involve several effects, and it is important to focus on the most relevant, i.e. the effect that is likely to trigger the most significant losses for the organization. To explaining the mean of CIA, in the context of risk analysis, the following rough breakdowns are presented [28]:

- Loss of Confidentiality - If the intention is to steel data.
- Loss of Availability - If the intention is prevent legitimate access to data.
- Loss of Integrity - If the intention is to cause harm by modifying data or systems.

Risk assessment

The next step in the FAIR ontology is to estimate each identified risk scenario. FAIR represents a risk estimation model which divides the estimation into components. The structure of estimating a risks significance is presented in Figure 2.4. The process of estimating risks shall start at the top (i.e. estimate a risk by estimating LEF and LM), and if necessary continue further down in the structure. A risk is considered necessary to be estimated in a lower level when valuable information regarding a risk's LEF and LM is absent. The FAIR ontology starts with the concept that risks equates to "Loss Exposure". The starting point therefore presents risk as:

The probable frequency and probable magnitude of future loss

According to FAIR ontology:

- Any analysis of risk must include both frequency and magnitude components in order to be meaningful.
- Since risk analysis is based on imperfect data and models, any statement of frequency or magnitude should be considered probability based.

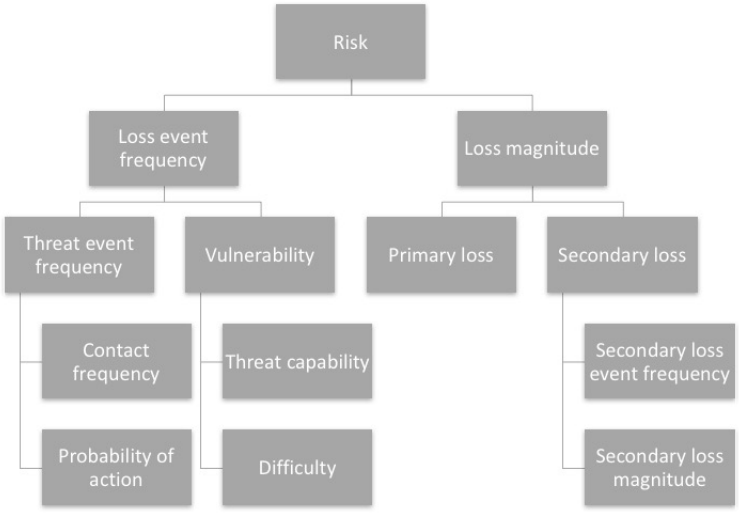

Figure 2.4: *The FAIR ontology.*

Given this, the first two factors, i.e. the first level of the decomposition of a risk, which risks are determined through are, see Figure 2.4:

- Loss event frequency (LEF).
- Loss magnitude (LM).

Loss event frequency, LEF

LEF is the probable frequency, within a given time-frame, that loss will materialize from a threat actor's action. The time-frame often used is annualized. LEF can be estimated directly or derived from Threat Event Frequency (TEF) and Vulnerability (Vuln). If LEF is estimated directly, participants estimate a minimum and a maximum value for how many times per year a threat will create losses within the organization.

TEF is the probable frequency, within a given time-frame, that threat actors will act in a manner that may results in loss. The key difference between LEF and TEF is that loss may or may not result from TEF. In order to estimate TEF the participants estimate a minimum and a maximum value for how many times (per year) a threat will expose the organization. TEF can be determined through Contact frequency (CF) and Probability of action (POF). CF is described as the probable frequency, within a given time-frame, that threat actors will come into contact with the assets. POF is described as the probability that a threat actor will act upon an asset once contact has occurred, hence try to harm the asset.

Vulnerability is the probability that a threat actor's action will result in a loss. Vulnerability represents a weakness that can be exploited, and is determined as a percentage representing the probability that a threat actor's action will result in loss. A minimum and a maximum percentage are estimated. For example: "The specific password is between 3-10% vulnerable to brute force attempts". Vulnerability can be determined through Threat capability (TC) and Difficulty (DIF). TC is described as the capability of a threat actor. Difficulty is described as the level of difficulty that a threat actor must overcome, i.e. by the organization implemented defences.

Table 2.2 presents an example of determinations of a risk's loss event frequencies.

Table 2.2: *An example of the threat event frequency, presented annualized.*

Risk ID	Minimum value	Maximum value
1	1	10
2	4	100
3	0,1	0,8

Loss Magnitude, LM

LM is the probable magnitude of primary and secondary loss resulting from an event. Therefore, LM represents the amount of tangible loss which is expected to be materialized from an event. Evaluating LM means determining whether losses falls into what are referred to as primary or secondary loss. In the FAIR ontology primary loss is considered as primary stakeholder losses that materialize directly as a result of an event. Primary stakeholders are those individuals or organizations whose perspective is the focus of the risk analysis. An example of a primary losses is monetary losses connected to the core business when it is unable to operate.

Secondary losses are considered losses that indirect affect the primary stakeholders. Indirect impact describes as secondary stakeholders (which are defined as anyone who is not a primary stakeholder that may be affected by the loss event) who react in a manner that further harms the primary stakeholders. An example of a secondary loss may be loss of reputation. The loss event might harm a customer of the organization. By the customer of the organization this loss event creates a negative reputation regarding the organization. Additionally, the customer stops buying services from the organization, making the organization decrease their sales.

There might occur several losses toward an asset from the current risk scenario being analyzed. Therefore, the decision of the LM should be decomposed into a Loss Type. These Loss Types shall be estimated individually, and in the end be summed up to a final value which represents the total LM for the risk scenario being estimated. The Loss Type can be of five different categories presented and described in the list below:

- **Productivity losses** are seen as primary losses and consist of two categories. Either losses that result from a reduction in an organization's ability to execute on its primary value proposition. A primary value proposition is the reason that the organization exists, usually as a result of the products and services that the organization offers the marketplace. Otherwise productivity losses result from personnel being paid but unable to perform their duties.
- **Response losses** are losses associated with managing the loss event. This loss form is often connected to primary losses and referred to as the time and money personnel needs to spend on managing the loss event.
- **Replacement losses** are often considered as primary losses and regard the costs of replacing the asset under question, e.g. replacing suffered physical asset.
- **Fine and judgement losses** are losses referred to as secondary losses. This type of loss occurs when a firm will get fined by a regulatory body, incur a judgment from a civil case, or pay a fee based on contractual stipulations.

- **Reputation losses** can occur when the reputation is damaged due to the Loss Event, and are seen as a secondary loss.

In order to determine a risk's LM, a minimum and a maximum value are decided. The minimum value represents the smallest probable loss that will affect the organization if the threat is successful. The maximum value represents the biggest probable loss that will affect the organization if the threat is successful. An example of an assessment regarding the loss magnitude of a risk is visible in Table 2.3.

Table 2.3: *An example of the loss magnitudes*

Risk ID	Loss category	Minimum value	Maximum value
1	Productivity	100h*$100	500h*$100
1	Reputation	$10000	$500000
2	Response	100h*$100	500h*$100

A quantitative risk analysis procedure provided by SANS Institute

SANS provides a quantitative risk analysis framework including of six stages.

- Conduct a risk assessment and vulnerability study to determine the risk factors.
- Based on the top 5 risk factors determined in the first stage, determine the value of assets under risk.
- Determine the historical attitude of the company under assessment in regards to their security practice for reporting loss incidents.
- Estimate the Annualized Rate of Occurrence (ARO) for each risk factor.
- Determine the countermeasures required to overcome each risk factor.
- Determine the Annualized Loss Expectancy (ALE) for each risk factor.

The following key variables and equations are used for conducting the quantitative risk analysis method provided by SANS institute [34]:

Exposure Factor (EF) = Percentage of asset loss caused by identified threat; ranges from 0 to 100%.

Single Loss Expectancy (SLE) = Asset Value x Exposure factor.

Annualized Rate of Occurrence (ARO) = Estimated frequency a threat will occur with in a year and is characterized on an annual basis.

Annualized Loss Expectancy (ALE) = Single Loss Expectancy x Annualized Rate of Occurrence.

Octave-Allegro (OA)

OCTAVE is a collection of tools, techniques, and methods for risk based information security assessments. There are currently three different methods for performing risk analysis provided by OCTAVE, where the most recently developed risk analysis method is OCTAVE-Allegro.

OCTAVE Allegro can be performed differently depending on requests from the organization where the analysis aims to be performed. OA can be performed in workshops, collaborative settings, and is also suited for those who want to perform risk assessment without extensive organizational involvement, expertise, or input. OCTAVE Allegro consists of eight steps:

- Establish risk measurement criteria - establish a way to measure risk based on the organizationsv́iew of risks.
- Develop an information asset profile - creating a priority list of information assets based on their importance to the organization.
- Identify information assets containers - where asset containers is information regarding the assets, such as data centers, assets owners, processes.
- Identify areas of concern - identify real-world conditions or situations that could affect the information asset.
- Identify threat scenarios - including asset, access, actor, motive, and outcome.
- Identify risks - creating a table for each asset where threat and its impact are listed.
- Analyze Risks - where the risks are analyzed based only on impact.
- Select mitigation approach - where each risk is given a ranking between 1 and four describing the need of mitigating the threat. During this step the probability of the threat is considered.

COBRA

COBRA is a developed program available to be downloaded for a fee. The program consists of two main parts namely:

- COBRA Risk Consultant.
- ISO Compliance.

Both of the sub-applications are customizable making the program usable for different types of organizations. The program uses expert knowledge to help customers identify and analyzing risks towards their business to manage information security related problems [16]. The Risk Consultant part consists of a digital questionnaire containing standard questions for gathering information regarding assets, vulnerabilities, threats, and current security controls of the organization. The program analyzing the data from the questionnaire and prioritize the threats based on their importance to be managed by the organization. Additionally, the program provides appropriate recommendations of alterations in order to mitigate the risks considered required. The probable losses connected to each identified risks is described both in terms of different types of losses and in monetary values for each loss type. The program is customized since it provides a customized knowledge base from where the program gather information. The Risk Consultant is designed to be self-analytic, enabling the software complete the risk assessment without expertise from the organization. The ISO Compliance comes with standard questions which assess the major categories specified in the ISO 27000 standard [1]. COBRA's standard processes are:

- Questionnaire building.
- Risk surveying.
- Report generation.

ISRAM

ISRAM is a paper-based quantitative risk analysis method. The method estimates risks based on their probability to occur and their following consequences. The method is considered paper-based since the approach includes conducting a survey where questions associated with the scope of the risk analysis are asked participants of the analysis. The method consists of seven steps which are presented in figure 2.5 [17].

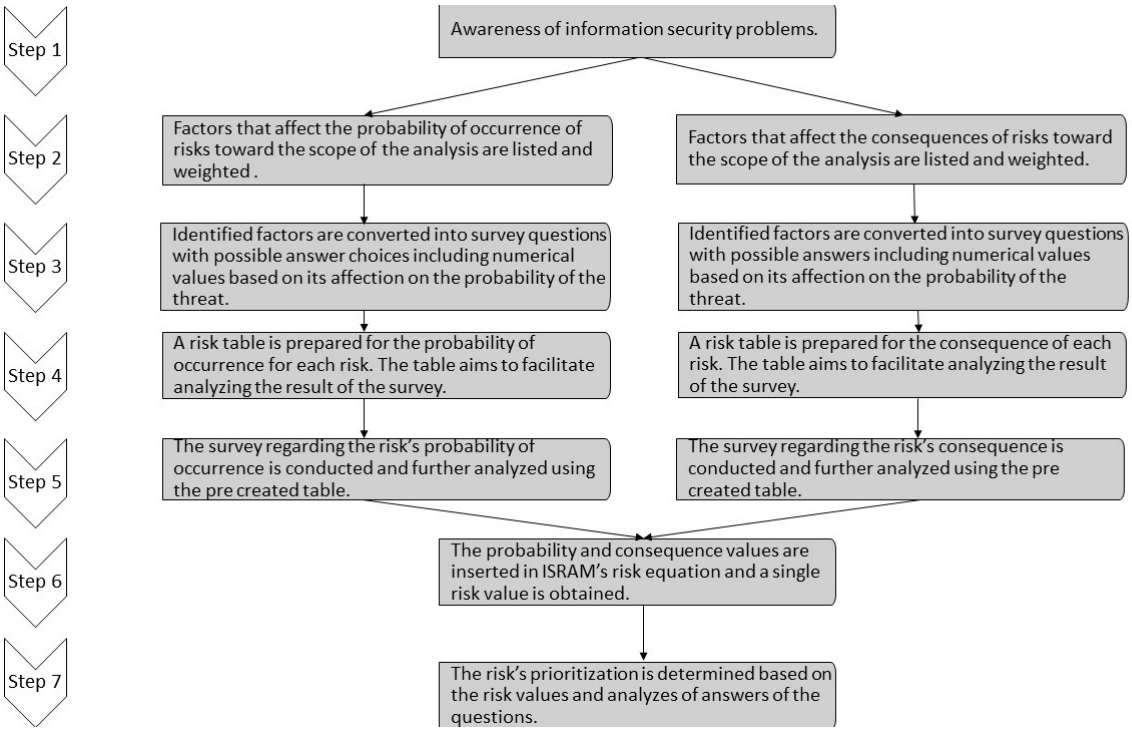

Figure 2.5: *Components of a risk according to FAIR.*

Mehari

Mehari is a risk analysis method which consists of consists four steps:

- Threat identification.
- Vulnerability identification.
- Risk determination.
- Final control recommendations.

In order to address relevant data for these four steps the method includes several actions vital to perform. These actions are:

- Developing security plans.
- Implementing security plans, or rules.
- Running light or detailed assessments of state of security.
- Risk evaluation and management.
- Ensuring the inclusion of security in the management of development projects.
- Security awareness and training sessions.
- Operational security management and the control/monitoring of committed actions.

The risk analysis method is knowledge based and requires experts from different part of the organization in order to assess valuable results [22, 36].

2.6 Monte Carlo

Monte Carlo methods are computational algorithms relying on repeated random sampling to obtain numerical results. The Monte Carlo methods vary, but in a high level tend to follow these particular pattern [2]:

- Define a domain of possible inputs.
- Generate inputs randomly from a probability distribution over the domain.
- Perform a deterministic computation on the inputs.
- Aggregate the results.

The essential idea is to solve issues that might be deterministic in principle by using randomness. Describing ranges, where the expected value of some random variable probably will be included in, enables to approximate this variable by taking the empirical mean of independent samples of the variable [2]. Monte Carlo method is preferable to use when modelling a phenomena with significant uncertainty in inputs, such as the calculation of a risk in a business. In risk analysis, Monte Carlo–based predictions of failure, cost overruns, and schedule overruns, are routinely better than human intuition or alternative "soft" methods [12].

Monte Carlo simulations enable to see all possible outcomes of the estimated risk, and therefor assess the risk's impact with considered to the uncertainty. When a Monte Carlo simulation is performed models of possible results are created. These models are created by substituting the estimated risk-values, i.e. the values which are described as a probability distribution, with the results from all Monte Carlo simulations. The Monte Carlo method calculates results as many times as the number of simulations are set to. Each time a simulation is performed, i.e. a result is calculated, the method uses different set of random values from the probability distribution range. In this way, Monte Carlo simulations provide a comprehensive view of what may happen. It tells you not only what could happen, but how likely it is to happen [9].

Monte Carlo simulation provides a number of advantages over deterministic, or "single-point estimation" analysis [2, 9]:

- Probabilistic Results - Results show not only what could happen, but how likely each outcome is.
- Graphical Results - Because of the data a Monte Carlo simulation generates, it is easy to create graphs of different outcomes and their chances of occurrence. This is important for communicating findings to other stakeholders.
- Sensitivity Analysis - With just a few cases, deterministic analysis makes it difficult to see which variables impact the outcome the most. In Monte Carlo simulation, it is easy to see which inputs had the biggest effect on bottom-line results.
- Scenario Analysis - In deterministic models, it is difficult to model different combinations of values for different inputs to see the effects of truly different scenarios. Using Monte Carlo simulation, analysts can see exactly which inputs had which values together when certain outcomes occurred. This is invaluable for pursuing further analysis.
- Correlation of Inputs - In Monte Carlo simulation, it is possible to model interdependent relationships between input variables. It is important for accuracy to represent how, in reality, when some factors goes up, others go up or down accordingly.

Using Monte Carlo simulation during risk analysis enables to show you many possible outcomes of the identified risks and tells you how likely they are to occur. It mathematically and objectively computes and tracks many different possible future scenarios, then describe the probabilities and risks associated with each different one. This means that it is possible to judge which risks can be accepted by the organization and which ones need to be avoided, allowing for the best decision making under uncertainty.

2.7 Program, Evaluation, and Review Technique, (PERT)

Estimating risks aim to reduce the uncertainty by structurally identify data and processes to predict and reduce future harm towards an organization. Depending on the approach of gathering and process data, the quality of the estimations will vary. When giving risks a "single-point" estimation, i.e. estimate a risk through one value only, the estimation will most certainly be wrong. Instead, providing a distributed range, i.e. a probability distribution, will increase the correctness of the estimation, and enables to quantify and accurately communicate uncertainty about the measurements [13]. By using probability distributions, variables can have different probabilities of different outcomes occurring. Probability distributions are a much more realistic way of describing uncertainty in variables of a risk analysis [9]. The PERT-model is based on giving a range of values where a minimum, a maximum and an expected value are provided. The PERT distribution is designed to generate a distribution that closely resembles realistic probability distributions since the PERT distribution emphasizes the "most likely" value over the minimum and maximum estimates. The PERT distribution constructs a smooth curve which gradually places greater emphasis on the values near the most likely value, in favor of the values around the edges. This process puts a lot of trust in the correctness of the estimated most likely value. Even if the estimated most likely value is not exactly accurate (as estimates seldom are), there is an expectation that the resulting value will be close to that estimate. Using PERT makes values around the most likely more likely to occur, still values between the most likely and the extremes are more likely to occur compared to many other probability distributions [9, 10]. Outcomes from PERT becomes input to Monte Carlo simulations where values are sampled at random from the input probability distributions. Each set of samples is called an iteration, and the resulting outcome from that sample is recorded. Monte Carlo simulation is performed over and over again depending on number of iterations the simulation is set to perform, and the result is a probability distribution of possible outcomes. In this way, Monte Carlo simulation provides a comprehensive view of what may happen. It tells you not only what could happen, but how likely it is to happen, based on expertise estimations.

2.8 Calibration

Calibration is a method for performing estimations that enables gauging and improving of a person's ability to estimate a risk effectively. A lot of risk analysis methods are highly dependent upon expert estimations. Calibration can be used when estimating a risk, in sense of estimating its probability and consequence, in order to avoid inherent biases and increasing the accuracy within the estimations. Calibration in risk analysis means using a range to estimate a risk's LEF or LM instead of a single point estimation. However, it is still necessary to make sure that the values used for estimating the ranges are as accurate as possible. To improve an estimation of a risk's probability range and consequence range a technique, presented by Douglas Hubbard, can be applied. The technique is based on constantly betting around the set limits for the risk's probability and consequence [13].

Humans tend to estimate better when money is on the line [9]. Furthermore, studies have shown that no real money is required for the process to have its desired effect on improving

estimations [9]. Another purpose of the usage of betting during estimations, is to have humans mentally weight the differences between their confidence in the range with a known level of confidence [12]. This mental weighting can be performed by including a "test" during the estimations. This test consists of including an imaginary profit sum. Participants can win this profit sum in one of two ways [12]:

- Participants can bet on whether their range contains the correct answer for a question.
- Participants can spin a wheel, where they win nine out of ten times.

The process of performing this test can end up in three ways [12]:

- The estimators will bet on their range. This means that they are more than 90% confident in their range. This being the case, they can and perhaps should narrowing their ranges until their confidence is lowered. If the range is not reduced, the used range might lack of a useful degree of precision, however narrow their ranges increases the risk of not providing accuracy in the ranges. There is always a trade-off between accuracy and precision within the process of estimating risks.
- The estimators will pick the wheel. In this scenario the estimators are less than 90% confident in their range, and should therefore expand the range to increase their confidence in the range. This further implicate that the degree of precision will deteriorate.
- The estimators cannot decide which option gives them the best odds. In this point the estimators have 90% confidence in their estimated range. Effectively the estimators have weighted a known 90% probability against their estimated range and founded them to be equivalent. The goal is to reach a 90% confidence in the estimated range in order to gain a convenient balance between the accuracy and precision within the result of the estimated risk.

3 Method

This chapter aims to describe the method of how the thesis was performed in order to respond to the research questions stated in Section 1.2. This includes how data was gathered and processed. Additionally how data was used in the implementation part, i.e. the selection and adaption of a quantitative risk analysis method, and finally evaluated.

3.1 Overview of approach

Part of the aim of this thesis was to evaluate the current qualitative method Secure State uses to perform risk analysis. The evaluation of their method enabled identifying both critical components important to maintain, as well as components having a negative impact on the precision and accuracy of the result. Furthermore, this study aimed to gather data regarding possible advantages of using a quantitative approach for conducting risk analysis. Additionally, an investigation of different quantitative risk analysis methods was performed and later on, the methods were evaluated based on their fulfillment of:

- Maintaining important components from the current method of Secure State.
- Improving the critical parts within the current method of Secure State.
- Including important components when performing quantitative risk analysis, identified during the literature review.

Furthermore, the quantitative risk analysis method that best suited the criteria was chosen and further used during a risk analysis at Secure State. In order to evaluate if the result was improved by using the presented method for conducting risk analysis, participants during the assessment answered a questionnaire regarding how the risk analysis was performed and how it affected the result.

In order to address the research questions proposed in Section 1.2, three consecutive tasks were performed, see Figure 3.1.

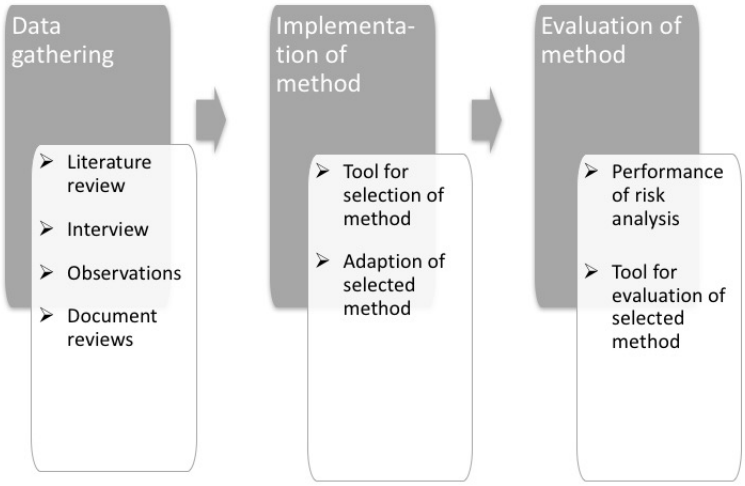

Figure 3.1: *Overview of the method.*

In order to respond to the first research question (see Section 1.2) the first task, called "Data gathering", involved observations of Secure State's current risk analysis method, interviews with employees of Secure State and reviewing documents from earlier risk analysis performed by Secure State. Furthermore, in order to address the first part of research question number two, namely "How can the result be improved by including quantitative measurements regarding risk assessment?", a literature review was conducted, where information regarding the performance of quantitative risk analyses and its accompanying challenges as well as possible effects on the results were extracted. Additionally, in order to gather the information required for performing the second task, where the second part of research question number two will be addressed, the literature review aimed to identify and provide knowledge regarding several quantitative risk analysis methods. Henceforth the first task will be referred as "Data gathering".

The second task, called "Implementation of method", aimed to address research question number two (see Section 1.2). The task involved evaluating quantitative risk analysis methodologies, identified in the literature review during the first task, in order to propose the most convenient method for achieving accuracy and precision within the result of a risk analysis. Requirements, necessary for the risk analysis method to fulfill, were identified based on the outcomes from the first task. These outcomes consisted of: advantageous components for the risk analysis method to include, parts within the current methodology of Secure State that were required to be improved, as well as important components in their method necessary to be maintained. The quantitative methods identified were evaluated based on their fulfillment of the requirements, where the method having the highest fulfillment of the criteria was selected.

In order to address research question number three (see Section 1.2), the third task, referred as "Evaluation of method", intended to evaluate the selected risk analysis method to see whether improvements, in terms of precision and accuracy of the results, were gained as well as to see if deficiencies in Secure State's previous risk analysis method were resolved. To evaluate the selected methodology for conducting risk analysis, the method was used during a risk assessment, where participants evaluated the method based on the performance and gained results.

3.2 Data gathering

In order to structure the process of gathering data during the observations, interview and review of documents, several questions were constructed in advance. The aim of these questions were to extract important information. The intentions of performing observations, interviews and document reviews were to identify how the current risk analysis used by Secure State is performed, its accompanying obstacles and furthermore how the obstacles affected the quality of the result. The questions were divided into two main parts:

- Mapping of the current situation.
- Selection and evaluation of a risk analysis method.

Questions marked with M are linked to "Mapping of the current situation" and questions marked with S are related to "Selection and evaluation of a risk analysis method". The first part, "Mapping of the current situation", i.e. question marked with M, were used as a starting point for gathering information during the observations and document reviews. The second part, "Selection and evaluation of a risk analysis method", i.e. questions marked with S, were used during the interview.

Mapping of the current situation

The following part describes the questions used as a basis for mapping the current situation regarding how Secure State conducting risk analysis, in which the various activities are investigated in order to identify weaknesses within their methodology. Mapping questions included in M1 are used to clarify the current methodology performed by Secure State.

- ***M1 What activities does the risk analysis performed by Secure State consist of, and how is results collected?***
- *M1.1 How is the scope determined?*
- *M1.2 Who participates during a risk analysis?*
- *M1.3 How are assets, connected to the scope, identified?*
- *M1.4 How are risks towards the assets identified?*
- *M1.5 How are the risks assessed, i.e. how is probability and consequence determined?*
- *M1.6 How is it decided whether a risk needs to be mitigated or not?*
- *M1.7 How are risks that needs to be managed prioritized?*
- *M1.8 How is measures to risks identified and selected?*
- *M1.9 How is it decided whether a risk becomes accepted given an implemented measure?*

Furthermore, to identify problems related to the approach of risk analysis taken by Secure State, that might affecting the results in an ambiguous way, mapping questions specified in M2 were used.

- ***M2 What problems exist in the current risk analysis model, and why does they occur?***
- *M2.1 Which parts of the risk analysis tends to be critical?*
- *M2.2 Are the assessments of risk values affected by group pressure?*
- *M2.3 Are any correlations of risks considered in the process?*

- *M2.4 Is the risk value calculated in a systematic manner?*
- *M2.5 Is the risk value based on reality?*
- *M2.6 Is the measured risk value based on logic?*
- *M2.7 Are available data taken into account, or is it only dependent on human estimations?*
- *M2.8 Dose the result obtain credibility?*
- *M2.9 Does the assessment provide dependability?*

Selection and evaluation of risk analysis method

The following part describes the questions that further were considered in order to choose and evaluate a quantitative risk analysis method. The purpose was to identify critical success factors, essential for the selected risk analysis method to include. Therefore, the following questions were specified in order to identify these critical success factors during an interview with the employee responsible for performing of risk analysis at Secure State.

- ***S1 Which activities are necessary to include in the method?***
- *S1.1 Which parts needs to be improved?*
- *S1.2 Which parts of the risk analysis are the most critical?*
- *S1.3 What is an improvement in your process of performing risk analysis?*
- *S1.4 Are there any parts of the process that needs to be remained, if so which ones, and why?*
- *S1.5 Are there any specific external requirements to consider, if so which ones, and why?*
- *S1.6 Are there any specific internal requirements to consider, if so which ones, and why?*
- *S1.7 What dose a good risk analysis consists of?*
- *S1.8 How should risk values be calculated?*
- *S1.9 How should probability and consequence be determined?*

Data assessment

Literature reviews

The literature review included to search in databases for written material, such as books, articles and journals. The literature used in the study were mainly scientific articles and subject-specific textbooks. To find scientific articles relevant for the study, searches through a service called UniSearch, available at Linköping University, were performed. UniSearch enables to reach materials available in the library, and in well-known databases available at the university, such as Scopus [4]. The search was structured according to a modified version of the approach presented by Rumsey and the following steps were performed [30]:

- Identify search terms
- Limit the search
- Truncation
- Combining terms (i.e. Boolean logic)

Firstly, words used for finding the information were identified, these words aimed to represent the ground for the search and consisted of significant words connected to the aim and subject of the study. The search words were identified by looking at the research questions of the study and further at formal designations of the concept of performing risk analysis methodologies. The search words were structured into matrices, where each column consisted of identified search terms and the rows is further different ways of expressing the initial term [30].

Secondly, requirements to limit the search were defined. Criteria used in order to limit the sources was language, only sources written in English or Swedish were included. Also the date of publication was considered before a source was used. The limit was set to only include sources published after 2010. However, if a good reason existed to why an older source was advantageous to be used, exceptions were taken, e.g. theory that has not been updated. The type of publication and further their number of citations were affecting the choice to obtain credibility in the study, though no predefined limits were set [30]. In order to save time and gather all sources connected to words having the same beginning, truncation was used. This made it possible to include all these words in the same query by using a specific symbol"*" as the remainder of the words where they were separated. On some occasions, in order to combine search words to be specific about what is wished to retrieve from the database, logic statements, called boolean connectors, were applied [30].

Tables 3.1, 3.2, 3.3, 3.4, and 3.5 presents the identified search words based on the process described above. Some boxes were left empty, since only relevant words connected to risk analysis were included.

Table 3.1: *How to perform quantitative risk analysis*

Concept	Perform	Quantitative	Risk analysis
Synonyms	Conduct, Implement, Execute, Follow out, Carry through		
Broad terms		Evaluation, Statistics	Risk assessment
Narrow terms		Quantification	Risk evaluation, Risk identification
Related terms		Monetary, Hybrid, Risk value	Consequence, Frequency, Probability, Likelihood, Risk value

Table 3.2: *Methods for identify and evaluate risks.*

Concept	Method	Identify	Evaluation	Risk
Synonyms	Approach, Methodology	Find, Discover, Detect, Address	Review	Hazard
Broad terms	Strategy		Review	
Narrow terms	FAIR, Octave, MCDM, NIST, LOPA		Estimate	Human, Cyber, Organizational
Related terms		Search for	Risk acceptance, Risk mitigation, Risk value Prioritize	Availability, Integrity, Confidentiality

Table 3.3: *Critics towards using qualitative risk analysis.*

Concept	Critics	Use	Qualitative
Synonyms	Criticism	Apply, Conduct	
Broad terms	Review, Opinion		Subjective
Narrow terms			Scoring methods
Related terms	Opponents		Expertise, Memory

Table 3.4: *Statistical measurement to address threats against information security.*

Concept	Statistics	Measurement	Threat	Information security
Synonyms		Calculation, Estimation	Danger, Hazard, Risk, Menace	
Broad terms	Scientifically	Determine, Decide, Evaluate	Uncertainty, Loss	Business, IT
Narrow terms	Tables/graphs of observed data, Numerals	Risk value	Spoofing, Hacking, Ddos	Availability, Confidentiality, Integrity
Related terms	Observation over time	Probability, Consequence	Harm	

Table 3.5: *Protection of assets.*

Concept	Protection	Asset
Synonyms	Defence	Resources
Broad terms	Safety	Primary assets, Secondary assets
Narrow terms	Prevention, Damaging	Information, Hardware, Software, Process, Stakeholders
Related terms		

Observations

Direct observations were conducted during two separate occasions, meaning that the observant was present, yet not participating during the risk analysis [38]. Information, based on the predefined questions marked with "M" (presented in the beginning of this section), was identified and documented during the whole observations.

Both observations were conducted at a client's head office located in Norrköping. The client had ordered two different executions of risk analysis, covering different departments and systems within the enterprise. The scope of the risk analysis and the participants present were therefore different during the two occasions. The purpose of the observations was to gather the information necessary to understand the current method and to get a deeper understanding of critical processes, its causes, and accompanying effects.

Document reviews

In addition to the previous method for collecting data connected to questions marked with "M", document reviews were applied. Document reviews meant reading through available documents that contained information from earlier performed risk analysis to access additional data of how Secure State performs risk analysis. The reviews were performed at Secure State's head office enabling access to all previous performed risk analysis. Since information regarding risk analysis is sensitive, only documented risk analysis by the client accepted to review were included.

Interviews

A semi-structured interview was performed to gather information to the questions (stated in the beginning of this section) marked with a "S". The respondent of the interview is specialized in risk analysis and responsible for how Secure State perform risk analysis. Additionally, the respondent acts analysis leader during most risk analysis performed by Secure State. The interview was performed at Secure State's head office, located in Norrköping. The interview was scheduled for one hour to enable extensive information gathering, still avoiding tiredness [20]. As an expert in the area, the respondent had both deep knowledge of risk analysis in general, such as their abilities and limitations, as well as in the risk analysis method used by Secure State. In order to collect and save information, documentations, in terms of notes, were taken during the whole interview.

3.3 Implementation of method

Identified information from the observations, interview and document reviews, regarding the critical components important for Secure State to maintain within the risk analysis method, as well as the parts having a negative impact on the result, were used in order to create criteria for the selection of a quantitative risk analysis method. Additionally, information gathered through the literature review, regarding performance of quantitative risk analysis and its influences on the result was also used for the creation of the criteria. Table 3.6 presents the framework for the selection of risk analysis. However, based on requirements from Secure State, there were some criteria that are demanded to be fulfilled by the risk analysis method in order to be selected. In Table 3.6 these criteria were marked with a "*". The quantitative method that resulted in the highest number of fulfilled criteria, given that all necessary criteria were fulfilled, was selected. If a method contained inadequate information regarding a criterion, the criterion was managed as if it was not fulfilled. The created criteria were:

- The method must have a quantitative approach.
- The method provide decision support, i.e. does the method provide mechanisms to mitigate necessary risks.
- The method needs to meet requirements of ISO 27000.
- The method use statistical data when available, but can still manage when no such data exists.
- The method needs to be "open source", i.e. provide free information with no requirements for licencing tools in order to enable applying the method.
- The risk analysis is performed during workshops.
- Human expertise are included in the assessment.
- The assessment is based on a logical approach, e.g. degradation of problems.
- There are sufficient documentation to extract necessary information regarding the method.
- The method is focusing on several problems during one occasion.

Each quantitative method, identified during the literature review, was evaluated based on its fulfillment of the criteria, where a:

- "x" means that the method fulfilled the criterion.
- "-" means that the method did not fulfilled the criterion.

Table 3.6: *Criteria for selection of risk analysis method*

Criteria	**Method 1**	**Method 2**	**Method n**
Quantitative*			
Decision support			
Meets Requirements of ISO 27000*			
Use statistical data, yet not dependent of it			
Open source*			
Assessment during workshops			
Uses human expertise			
Logical approach (i.e. breaking down problems)			
Enough available information*			
Focus on several problems			

- " " means that information regarding that criterion was absent.

Additionally, the selected method was further adapted to keep some practicality within the current approach of Secure State. The adjustments meant that the risk analysis was going to be performed in a workshop, having necessary participants from the client present. Furthermore, the method was divided into two parts, firstly identification and assessment of risks, and secondly identification and assessment of alterations toward risks evaluated as in need of mitigation.

3.4 Evaluation of method

The third task aimed to evaluate the chosen risk analysis method, to see whether improvements of the result in terms of accuracy and precision were gained, and previous deficiencies within the method used by Secure State were resolved. In order to evaluate the selected methodology for conducting risk analysis, the method was used during a risk assessment, where participants evaluated the method based on the performance and gained results. There were four participants present excluding the analysis leader. Three of four participants were familiar with the current way of performing risk analysis at Secure State, where one is the responsible for the process of conducting risk analysis at Secure State. The fourth participant did not have previous experience within Secure State's risk analysis method. However, the participant had a broad knowledge and experience within information technology security in general. The analysis regarded risks related to Secure State's internal SOC-service. The assessment was scheduled for five hours, and aimed to identify and evaluate risks and measures responding to supplying intrusion detection services (IDS) and beneficial responses for customers to Secure State.

The evaluation of the performed risk analysis was based on a questionnaire. How the questionnaire was performed was inspired by "The System Usability Scale" (SUS) [35]. All statements of the questionnaire provided by SUS was change to be appropriate for this specific thesis. According to the SUS questionnaire each claim was either positively or negatively targeted. All odd numbered claims were positively targeted and all even numbered claims were negatively targeted. This in order to avoid only evaluating the method based on a positive or a negative attitude. Furthermore, according to SUS ten claims were created for the questionnaire. The questionnaire consisted of ten claims, these claims were meant to be rated based on how much the respondent agreed to them. As with SUS, the rating consisted of a five-graded scale: from Strongly agree to Strongly disagree. The following claims were asked to be judged:

1. By setting a maximum and minimum value, the "correct value" were most certainly covered.
2. Dividing the risks into smaller components (asset at risk, threat community, threat type, effect and loss form) were complex and arbitrary.
3. Breaking down the risk into smaller components often made it possible to find useful information in order to understand and estimate the risks.
4. The evaluation of risks was based on opinions rather then statistics of similar risks.
5. Apply Monte Carlo simulations in order to randomly model different outcomes, based on each risks defined weighting, is preferable in order to take uncertainty into consideration.
6. Dividing the risks into smaller components (asset at risk, threat community, threat type, effect and loss form) resulted in unnecessary work and less participation within the assessment group.
7. Base the estimation of an annualized frequency to determining the probability, and a loss magnitude to determining the consequence, decreased the arbitrariness of the decision.
8. By using PERT-analysis to estimate the maximum, minimum and most likely values of a risks probability and consequence, were unclear and hard to understand.
9. Decisions were discussed and based on the groups common opinion.
10. Estimating a risks probability and consequence further down in the pyramid than LEF and LM (i.e. loss event*vuln, primary and secondary losses) was considered complex.

In order to interpret the results of the questionnaire, an approach inspired by the SUS-evaluation was applied. The grading number participants gave each claim, based on how much they agreed with the claim, was converted into a new number [35]:

- For odd-numbered items: subtract one from the user response.
- For even-numbered items: subtract the user response from five.

This provided each of the graded claims with a new number between zero and four, where a four presented the most positive response. A four is representing the most positive response for negative targeted claims due to the conversion being made where the user response was subtracted from a value of five. A four is also representing the most positive response for claims with odd number. This since the user response was subtracted with one. The converted values for each claim connected to one person were summed, this sum (of the converted values) becomes a value between 0-40. The results of the questionnaire can both tell which claims the participants agreed to the most as well as an overall score for how good the participants thought the method was according to the claims. A value near to 40 would indicate that the proposed quantitative method would be an improvement according to the respondents. A value of 20 would indicate that the method is neither better nor worse than the currently used method by Secure state. And a value below 20 would indicate that a change of method is not advantageously according to the respondents. The claims is based on the changes that was made by introducing the quantitative risk analysis compared to the currently used method. These changes were processes which aimed to improve the currently used method. Therefore, if the participants considering these processes useful, the proposed quantitative method would be a good alternative for Secure State to apply when performing risk analysis.

4 Results

This chapter presents the results of this study. The results are divided into three parts, which follows the structure of how the results were gathered, see Chapter 3. These three parts are: Section 4.1 Data gathering, 4.2 Implementation of method, and 4.4 Evaluation of method. Section 4.1 presents the results gained during the data gathering, i.e. the results regarding Secure State's currently performed qualitative risk analysis method. Section 4.1 includes a description of Secure State's currently used risk analysis method, its advantages, and its disadvantages. Section 4.2 describes the quantitative risk analysis method created for Secure State to use during risk analysis. Section 4.4 presents the result of the evaluation of the presented quantitative risk analysis method.

4.1 Data gathering

The results gathered for this section is based on interviews on employees at Secure State, observations during risk analysis conducted by Secure State, and data reviews of documentations from earlier performed risk analysis by Secure State. Worth noticing is that the information provided during this section is referring to how Secure State performs and perceive risk analysis, not according to scientific sources.

Clients order a risk analysis from Secure State, and the analysis is often held on two separate occasions, or at least divided into two main parts. The first part constitutes of addressing risks and its consequences towards the business. The second part focuses on identifying measures toward the identified risks. The measures aim to ensure that consequences, from a non-accepted risk, will decrease to a point where the business can accept the risk. A participant from Secure State is acting as the risk analysis leader, where Secure State provides knowledge and expertise within the concept of risk analysis, enabling to gain desirable results. Participants from Secure State are also responsible for compiling the outcome of the risk analysis into a proposition of what the client should do in order to put the object, i.e. the scope of the risk analysis into a "safe state". A "safe state" refers to the situation where risks considered critical towards the scope of the analysis are mitigated. The risks shall then be managed to a point where the risk's impact towards the organization has decreased to an acceptable level.

Framework of method used by Secure State

The method used by Secure State meets the requirements from the 27005 standard. The overall processes of risk analysis performed by Secure State are presented in Figure 4.1.

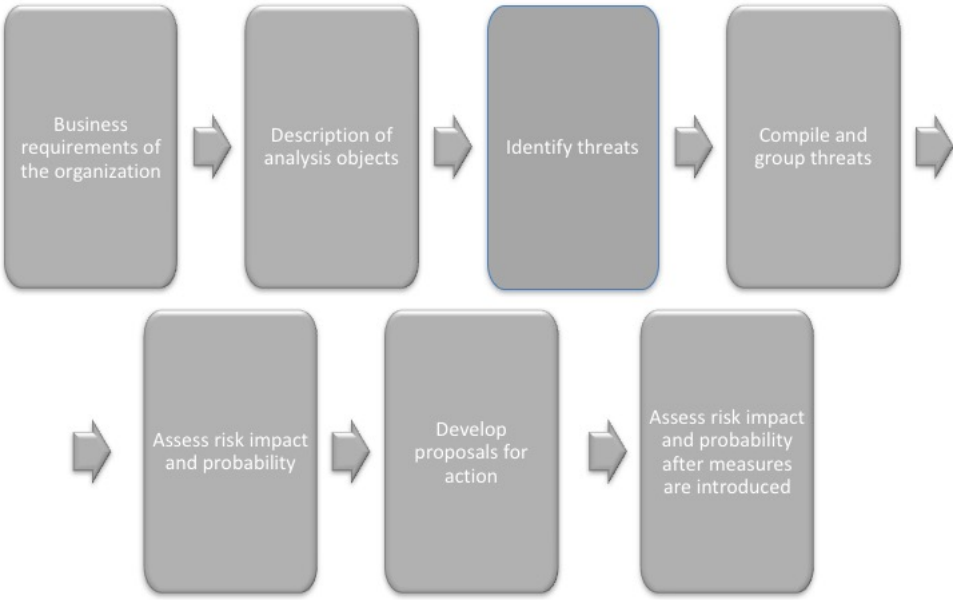

Figure 4.1: *The overall processes of a risk analysis preformed by Secure State.*

The risk analysis performed by Secure State consists of two main parts. The first part regards identifying risks and evaluate their likelihood and consequence. The likelihood and consequence of a risk are combined in order to determine a risk value. The given risk value enables prioritization of the risks in order to identify the risks that pose the greatest threat towards the organization. During the second part, action proposals for risks in need of mitigation are identified. Given an implemented measure, a new evaluation regarding the risk's impact on the business is performed.

Participants during a risk analysis

Secure State has clients operating in a broad field of different businesses, where contract and agreements for the risk analysis are different in terms of time period, scope and area. Secure State has therefore both experienced customers as well as customers having a small understanding towards the process of performing risk analysis. Employees at Secure State are leading the risk analysis ordered from their clients. A risk analysis requires expertise within different areas connected to the scope of the risk analysis. Therefore, it is important that the participants during the risk analysis consists of a selection of people with enough expertise in all fields connected to the scope of the risk analysis. During the process of performing the quantitative risk analysis used by Secure State the following roles are required to be involved:

- **Responsible client** - this is the person that initiates the risk analysis.
- **The analysis leader** - this is the person leading the risk analysis from Secure State. The initial work for the analysis leader is to gather an understanding of the result which the

client expecting. Understanding the expected results enable to create an understanding of the task.

- **Experts of various kinds** - depending on the type of risk analysis different positions are required, such as IT engineers, safety coordinators, and lawyers. These are the persons having knowledge regarding the object or process which constitutes the scope of the risk analysis. Together with the support from Secure State, these experts identify risks and further interventions.
- **Employees** - are persons having a business perspective on the object that is being analyzed and are important include in the assessment group.
- **Documentation manager** - this position is covered by Secure State. The documentation manager documenting all information of interest during the risk analysis. Secure State further uses the notes for creating action plans based on the result from the risk analysis.

The analysis group can vary regarding size depending on the risk analysis and its scope, but according to Secure State the analysis group should not be to big in order to perform a structured assessment. However, the size of the group is not what is most important, rather what persons that are participating, i.e. what knowledge that are present during the risk analysis. It is important that the group has adequate resources, powers, and that necessary administrative support is in place. Secure State often encounters problems regarding the wrong participants, e.g. only having technicians or people who do not know enough about the business participating. Inputs regarding the business might in this situation, i.e. situations where participants having knowledge of the business perspective are missing, become inadequate and the risk analysis might not identify measures of risks reflecting the need of the organization as a whole. Another problem often occurring within the group performing the risk analysis is that some participants tend to dominate the assessment. Having people dominating the risk analysis makes other participants find it hard to contribute with their knowledge, which might result in inadequate information provided. Suggestions regarding risks and their estimations from the person dominating the group tend to end up as the result, making the assessment be based on the loudest person, rather than expertise. The main task of the analysis leader is to bring everyone into the discussion and make the analysis group focus on the "right" risks, i.e. the risks which constitute the biggest threats toward the organization.

Identification of risks

During a workshop where a risk analysis is held, the person acting analysis leader ensures that the risk analysis group understands each other and the scope of the risk analysis and moving forward in the assessment. It is important to ensure that the analysis group is of the right composition and that the scope of the risk analysis is clear and limited. All participants need to understand the assignment and their own task, as well as being aware of the value of their participation. The analysis leader from Secure State has the responsibility to lead the risk analysis and further encourage the assessment group to dare to be active. Secure State often encounters groups of participants having a low commitment, and rather see the risk analysis as something to be discarded. To ensure that the scope of the risk analysis is clear, Secure State's responsibility towards the client is to help them initialize clear tasks with clear demarcations.

The scope of the risk analysis is the object or the process that the client has ordered the risk analysis for. The initial task during a risk analysis is a description of the scope for the risk analysis. The responsible person from the client, i.e. the person who ordered the risk analysis, presents the scope of the risk analysis, including clear limitations. A discussion among the group initializes where the group sort out problems and misunderstandings, to make sure that the whole assessment group understands the scope and the intention of the

risk analysis. This part, i.e. understand the scope and its limitations, tends to be problematic. Clients often face problems regarding defining the scope and set limitations. Therefore, a risk analysis often begins with long discussions before the actual assessment of risks can begin.

After the scope has become clear towards the risk analysis group it is time to start gathering data into the risk analysis. Each member in the assessment group writes down all possible risks, related to the examined object, on separate papers. The risks are then presented by the analysis leader, who at the same time groups similar risks to structure the process. Risks judged to be out of scope are removed. All paper are put on the wall as they are grouped in order to always be visible to the participants. During the grouping, new risks may be identified and included. Since everyone starts identifying the risks individually, each persons' thoughts regarding potential threats will be taken into consideration, making this part be less dependent on the environment of the group. For instance participants do not need to compete in order to make their opinion heard. The identified risks are completely based on the persons operating in the workshop, hence the importance of having a broad field of knowledge becomes clear here.

Evaluation of risks

When the risks are identified and grouped the next step is to score the risks based on their likelihood of occurrence and consequence. This part aims to determine whether it is necessary to mitigate the risks or not. The evaluation of the risks, i.e. determining a likelihood value and a consequence value for each risk, is performed as an open discussion with the aim of jointly determining the risk value of each risk. The decisions should be based on two main criteria:

- How likely the threat is realized.
- What the threat's consequences will be if realized.

The grading scale used for determining the likelihood and consequence value consists of a number between one and four. Table 4.1 and Table 4.2 gives a general description of the probability levels respective consequence levels within the two scales.

Table 4.1: *The scale used for determining probability of a threat*

Number	Probability	Description
1	Unlikely	An event that is considered unlikely to occur within a 5-year period.
2	Quite unlikely	An event that is expected to occur rarely, no more than once a year.
3	Likely	An event that is likely to occur. Occurs up to a few times a year.
4	Very Likely	An event that is most likely to occur. Occurs very often/daily.

Table 4.2: *The scale used for determining consequence of a threat*

Number	Consequence	Description
1	Negligible	An event that negligently negatively affects the business and its assets.
2	Minor	An event that has a slight negative impact on the business and its assets.
3	Considerable	An event that has a significant negative impact on the business and its assets.
4	Serious	An event that has a serious negative impact on the business and its assets.

Everyone having an opinion regarding the grading should announce it. The group discusses the proposed values towards a common decision, resulting in one probability value, i.e. a number which describing the probability of the risk and one consequence value, i.e. a number which describing the consequences of the risk. The risk value is measured by multiplying these two values, i.e. the probability and consequence values. The risks are placed into a risk matrix based on their risk values. The possibility values are placed on the horizontal axis and the consequence values on the vertical axis, see Figure 4.2. This matrix, see Figure 4.2, gives a clear view of how risks are prioritized in sense of which risks to manage, and in what order.

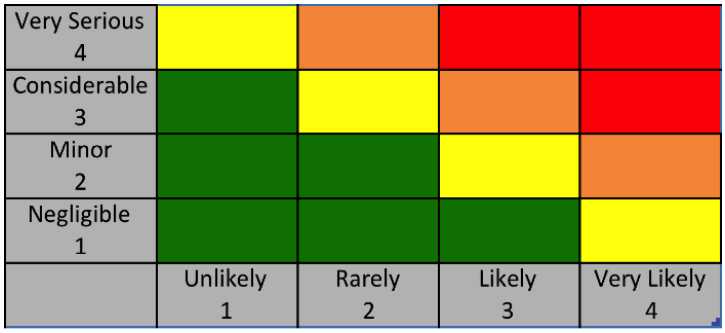

Figure 4.2: *The risk matrix used by Secure State.*

The decision of each risk's probability and consequence value tends to become arbitrary since a motivation to why the decision is taken often are missing. The choice of values for the consequence respective probability often turns out to be dependent on human beliefs rather than actual conditions, i.e. the information behind the decision are usually inadequate. Furthermore, the assessment of risk values are commonly influenced by group pressure as well as of the first estimation mentioned. The first estimation mentioned regarding a risk's probability and consequence are commonly accepted without deeper investigations regarding its

credibility, i.e. investigations regarding the actual condition to why the value was considered appropriate. Furthermore, the meaning of each grade within the probability scale and the consequence scale are interpreted differently by different participants, therefore the estimations of risk values tend to become arbitrary. A definition of what each grade in the probability respective consequence scale means is available, see Table 4.1 and 4.2. However, the definition of each grade within these scales is only presented briefly in the beginning of the assessment and tends to not be considered during the actual determination of a risk's probability value and consequence value.

Risk mitigation

The second part of the risk analysis is about deciding action plans for how to mitigate risks. The participants write down their action proposals to respective risk, placed in either the red, orange, or yellow box in the risk matrix presented in Figure 4.2. If a risk is placed in a green box in the risk matrix the risk is considered accepted by the organization and therefore is no need to mitigate the risk. The action proposals are discussed in the group, with the aim of identifying the most appropriate measures for each risk. The intention is to identify both preventive and anti-corruption measures. Preventive measures aims to obstruct the risk to materializes while anti-corruption measures aims to reduce the consequence if the risk is materialized. Given implemented measures, a re-evaluation of the risk's risk value is performed. The new risk values are repositioned in the risk matrix. Repositioned risk values aim to ensure that each risk has decreased either by prevention or harm reduction, and are now placed in one of the green boxes in the risk matrix, i.e. accepted by the organization.

Areas of concern

To sum up, the following list presents areas of concern during risk analysis performed by Secure State:

- Bias within the grading system.
- Arbitrariness in the evaluation system.
- Difficult to understand the scaling system.
- Limited competence of participants.
- Difficulty to define or describe the scope for the analysis.
- Some participants tend to "take over" the discussion.
- Low commitments (risk analysis are seen as something to be discarded).
- Hard to focus on the "right" risks.
- Not using available statistics data.
- Decision tend to be based on thoughts rather than facts.

4.2 Implementation of method

The quantitative risk analysis methods identified were (for a short introduction to each one see Section 2.5)

- A quantitative risk analysis procedure provided by SANS Institute (SANS) [34].
- OCTAVE-Allegro (OA) [7].

- Mehari [22, 36].
- COBRA [1].
- ISRAM [17].
- FAIR [9].

Table 4.3 presents the criteria fulfilled by each of the five methods being investigated.

Table 4.3: *Evaluation of quantitative methods.*

Criterias	**SANS**	**OA**	**Mehari**	**COBRA**	**ISRAM**	**FAIR**
Quantitative*	x	x	x	x	x	x
High decision support	x	-	-	x	-	-
Meets Requirements of ISO 27000*	x	x	x	x	x	x
Use statistical data, yet not dependent of it	x	-	x	-	x	x
Open source*	x	x	x	-	x	x
Assessment during workshops	x	x	x	x	x	x
Uses human expertise	x	x	x	x	x	x
Logical approach (i.e. breaking down problems)	x	-	x	x	-	x
Enough available information*	-	-	-	x	x	x
Focus on several problems	x	x	x	-	-	x
Sum of fulfilled criteria	8	8	8	7	7	9
Fulfilled all required criteria	-	-	-	-	x	x

Quantitative risk analysis method selected

FAIR was selected as the method to be introduced to Secure State, based on the result from Table 4.3. FAIR fulfilled all except one criterion, which gave FAIR the highest fulfillment of the criteria. FAIR did also fulfill all criteria required to be fulfilled. However, some modifications of the selected method was made in order to be appropriate for Secure State. These modifications are described in Section 4.3.

FAIR is a method based on objective inputs making the risk analysis fulfill the criteria of being a quantitative risk analysis method. Additionally, since the method relying on objective inputs, the results becomes very defensible and repeatable [33]. The method do not provide high decision support since the method initially did not include any process of identifying alterations toward the risks considered as in need of mitigation. The quality of the results gathered during the risk analysis increases as more relevant statistical data is gathered, however if clients do not want spending time on gathering statistical data the method do not require identifying statistical data. A strong recommendation is however to spend resources on assessing statistical data to increase the possibility of assessing results containing both good precision as well as obtained accuracy. In order to perform the method there are no licences or programs that needs to be bought. FAIR provides software making it easier to structure the assessment as well as performing included measurements. However this software is not required, it is easy to structure an assessment according to FAIR only having excel installed on the device. This might requires a fee, however it is not specific for the risk assessment and MS Office is already utilized at Secure State. Additionally, there are add-ins available for excel in order to perform Monte Carlo simulations using PERT as inputs, or it is possible to easily build your own Monte Carlo simulator in excel. The framework of FAIR requires that expertise are participating during the assessments, i.e. the method uses human expertise. How and where the assessments should be performed is not strictly stated in the framework, and a workshop would be highly suitable for identifying

and assessing risks. The FAIR method have a logical approach since it divides risks into smaller components. Decompose the risks makes it easier to understand the risks, see how vulnerable the organization might be towards the risks, identify how it might harm the organization and how to mitigate the risks. Finally the method enables focusing on several risks in the same assessment. The process of identifying, decompose, and estimate risks can proceed until there are no more risks identified. Of course as more risks are being identified and estimated as more time requires to be spend on the analysis [9].

4.3 Methodology explanation

The proposed quantitative method, is presented during this section. As described during the explanation of method used for this thesis, see Chapter 3, the selected method was adapted to include components within the current method used by Secure State. These components included several processes worth establishing within the new FAIR inspired risk analysis method, namely:

- The current process of preforming risk analysis in workshops.
- The current process of identifying and grouping risks included in the scope.
- The current process of identify measures.
- The current process of measure risks given implemented measures.

The FAIR-inspired risk analysis method is divided into six different steps. Figure 4.3 gives an overview of these six steps, and the following section aims to describe these steps and provide an understanding towards the proposed method.

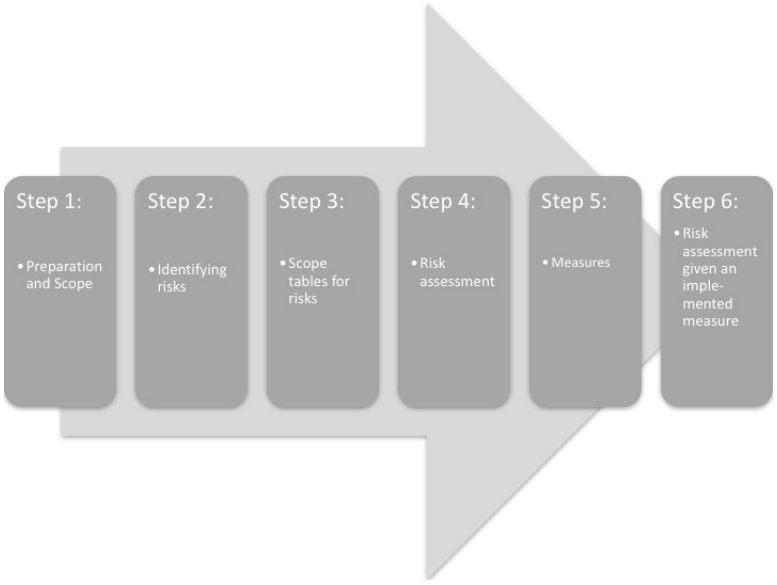

Figure 4.3: *An overview of the six different steps within the proposed quantitative method.*

Step 1: Preparation and scope

The scope of the risk analysis shall be presented with clear definitions of what is expected and limits of the risk analysis. The scope shall be presented from the client in the initial part of the risk analysis. The risk analysis will be performed during a workshop, where necessary participants having the required expertise shall be present. This step will be performed

accordingly to Secure State's currently approach. This means that the responsible client is responsible for provide a clear scope toward the rest of the assessment group. During this part the rest of the assessment groups are encourage to ask questions in order to create a common understanding of the scope and its limitations.

Step 2: Identifying risks

To identify risks, participants individually write down their own identified risk towards the scope of the risk analysis on papers, one risk per paper. Depending on the risk analysis, in terms of scope, participants, and organization, the time required for this step will differ.

Furthermore, the analysis leader collects, presents, and in accordance with inputs from the participants, groups each risk while placing them visible for the assessment group. Risks are grouped if they are considered similar, i.e. having similar threat communities and threatens similar assets. A threat community can be seen as the type of threat actor, and will be described further during step three. Each group shall then be given a risk identification (ID) number. If duplicates or risks out of scope are identified, they shall at this point be excluded from the analysis. This step follows the framework of how Secure State currently identifies risks and reused in the presented quantitative risk analysis method.

Step 3: Scope tables for risks

Each group of risks shall from this point be managed separately, hence the rest of the method shall be performed several times depending on the number of identified and included groups of risks. Henceforth, each group of risks are referred to only as a risk. The aim is to create a "scope-table" for each risk, see Table 4.4. These "scope-tables" intend to divide the risk into four different components, which are presented in the list below. The process of creating scope-tables and decompose the risks is based on the FAIR-method.

- Asset at risk, e.g. customer information, company information, company process, or money at an account.
- Threat community, e.g. privileged insiders, non-privileged insiders, cyber criminals, or customers.
- Threat type, e.g. malicious, accidental, error, or fraud.
- Effect, e.g. confidentiality, integrity, or availability.

Each risk might, for example, affect several assets, based on different threat types, having different effects on the asset. Each of these combinations of the components stated above, connected to one risk, is called a risk scenario. Therefore, each risk may consist of several risk scenarios. To decide whether a risk needs to be divided into several scenarios, a rough estimation whether the probability or consequence of the scenarios is likely to differ. If so, they shall be divided into several risk scenarios and be managed separately. As an example, the first risk in Table 4.4 is divided into three scenarios. Each risk scenario, connected to the first risk in Table 4.4, is given a decimal number in order to separate the risk scenarios. Otherwise, i.e. risk scenarios having the same probability and the same consequence, the risk can be managed as one scenario. All significant scenarios need to be evaluated in order to estimate the probable consequence and probability of a risk. Each row in Table 4.4 presents a distinct risk scenario, required to be analyzed.

Table 4.4: *Example of a scope table for risk associated with each risk ID.*

Risk ID	Asset at risk	Threat Community	Threat type	Effect
1.1	Customer information	Privileged insiders	Malicious	Confidentiality
1.2	Customer information	Privileged insiders	Accidental	Confidentiality
1.3	Customer information	Non-privileged insiders	Malicious	Confidentiality
2	Customer information	Cyber criminals	Malicious	Confidentiality

Step 4: Risk assessment

Each risk scenario is further evaluated and given a Loss Event Frequency (LEF) and a Loss Magnitude (LM). The meaning of LEF and LM will be described in the next sections. However, important for the estimations of LEF and LM is to use data based on statistics of similar events. LEF and LM shall be determined by estimating a range of possible values, including a minimum value, a maximum value, and an expected value. All these values should be identified based on statistics available. This estimated range shall further be performed in a calibrated manner, see Section 2.8. Figure 4.4 presents an overview of how to estimate a risk within the selected and modified quantitative risk analysis. Give each risk a LEF and a LM and further use calibration is based on the FAIR-approach.

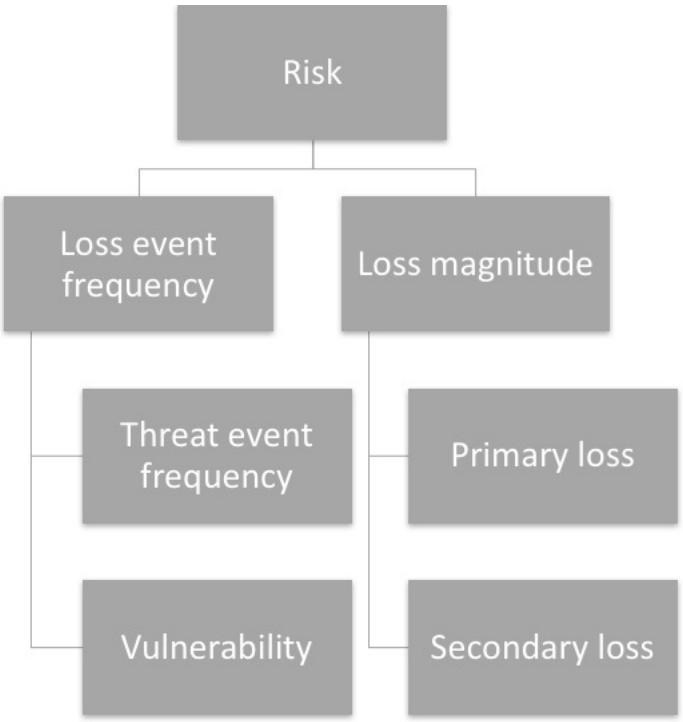

Figure 4.4: *The framework for estimate the risk, an modified version of the original framework in FAIR ontology.*

Loss event frequency (LEF)

LEF is the probable frequency, within a given time-frame, that loss will materialize from a threat actor's action. The time frame used is annual. Using an annual time frame dose not affect the result, it is just to present the value in a consistent way so it is easy to relate. Hence, if a risk is likely to occur one time in two year (as its minimum value) the annual value shall be 0,5. LEF can be estimated directly or derived from Threat Event Frequency (TEF) and

Vulnerability (Vuln), see Figure 4.4. If statistics can provide information regarding LEF directly, that estimation should be performed. Going one level down in Figure 4.4, i.e. estimate TEF and Vuln often becomes more complex than it make the estimation easier. However, if sufficient information cannot be found in order to estimate LEF, statistics regarding a risk's TEF and Vuln might be available. If so, the estimation should be based on TEF and Vuln. To estimate LEF, a minimum LEF, a maximum LEF, and a most likely LEF are determined, where each estimation represents the annualized value.

TEF is the probable frequency, within a given time-frame, that threat actors will act in a manner that may result in loss. The key difference between LEF and TEF is that loss may or may not result from TEF.

Vulnerability is the probability that a threat actor's actions will result in loss. Vulnerability represent a weakness that can be exploited, and is determined as a percentage representing the probability that a threat actor's actions will result in loss. For example: "The specific password is 3% vulnerable to brute force attempts".

Table 4.5 presents an example of how the LEF could be estimated and further documented.

Table 4.5: *An example of determined and documented LEF within an annualized time-frame.*

Risk ID	Minimum value	Maximum value	Most likely value
1	0,5	2	1
1	0,8	3	2
1	1	10	3
2	0,1	1	0,5

Loss Magnitude (LM)

LM is the probable magnitude of primary and secondary loss resulting from an event. The LM is about how much tangible loss is expected to materialize from an event. Evaluating LM includes to determining whether losses fall into what are referred to as primary or secondary loss. Primary loss is considered primary stakeholder loss that materializes directly as a result of an event. Primary stakeholders are those individuals or organizations whose perspective is the focus of the risk analysis.

Secondary loss is the primary stakeholders loss-exposure that exists due to secondary stakeholders reaction to the primary event. Secondary stakeholders are defined as anyone, who is not a primary stakeholder, that may be affected by the loss event being analyzed, and react in a manner that further harms the primary stakeholder.

There might be several losses identified toward an asset for the risk scenario being analyzed. Therefore, the decision of the LM for each loss identified, should be decomposed into loss type. These loss types shall be estimated separately, and in the end be summed into a final value. The loss types can be of five different categories presented in the list below:

- Productivity losses
- Response losses
- Replacement losses
- Fines and judgment losses
- Reputation losses

For further description of each loss type see Section 2.5.

Table 4.6 presents an example of how the LM is assessed and documented.

Table 4.6: *An example of determined and documented LM.*

Risk ID	Loss Type	Minimum value	Maximum value	Most likely value
1.1	Productivity	100h*$100	500h*$100	200h*$100
1.2	Reputation	$10K	$50K	$30K
1.3	Response	8h*$100	100h*$100	16h*$100
2	Productivity	4h*$100	20h*$100	8h*$100

Measurement

According to the FAIR-method, the calibrated ranges of LEF and LM for each risk are used for the selected probability distribution method called PERT (see Section 2.7). The results from the PERT method is then used as input to the Monte Carlo method, (see Section 2.6). The Monte Carlo method is used in order to simulate the PERT distribution 1000 times. There

is possible change the number of simulation, but according to the FAIR methodology one should not have to few simulation in order to utilize the positive outcome by including Monte Carlo simulations, hence it is not preferable have a lower number than 1000 simulations [9]. The outcome from the usage of Monte Carlo method (over the defined domain of possible inputs) can be interpreted by placing the result of each Monte Carlo estimation in a "heat map". Figure 4.5 represents an example of a possible "heat map" where four risks (the points placed in the chart) are placed in the mean of each risk's distributed result.

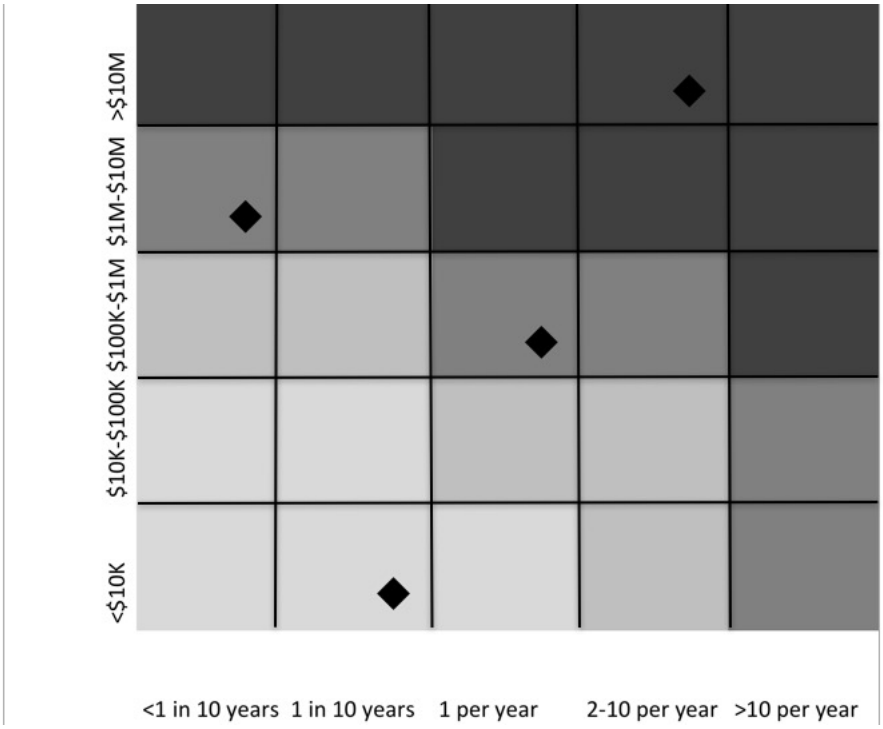

Figure 4.5: *An example of a "heat map" used for interpreting results from the Monte Carlo method, where PERT is used for distribute the input, i.e. the probability distribution.*

Using Monte Carlo simulations where inputs is based on estimations made by using PERT, the analysis will be based on random estimates for each estimation. This will produce a model that takes into account variability, for each risk independently. As described earlier, the input to the PERT distribution consists of a estimated minimum, maximum, and most likely value. The output, i.e. what the PERT distribution returns, is a sample from that distribution. The distribution creates a smooth curve, Figure 4.6 provides an example of a PERT distribution.

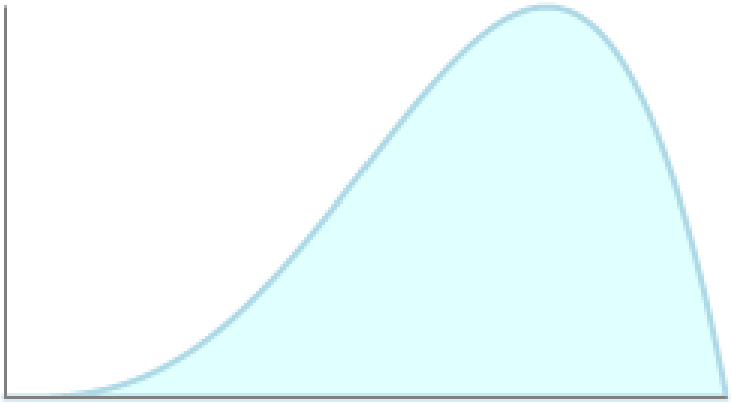

Figure 4.6: *Examples of the PERT distribution, a smooth curve. Values near the peak are more likely than values near the edges.*

PERT is designed to generate a distribution that closely resembles realistic probability distribution, therefore the most likely value is used. The PERT distribution emphasizes the most likely value over the minimum and maximum estimates. However, the PERT distribution constructs a smooth curve which places progressively more emphasis on values near the most likely value, in favor of values around the edges. In practise this means that we believe the estimation of the most likely value. Still, estimations of the future can never be exactly accurate making it useful to use inputs from the whole estimated ranges.

From these estimated ranges Monte Carlo simulations can run. In practise, a Monte Carlo analysis means to run the same PERT-model but thousands of times. Each time a simulation runs the value is recorded. When all simulations is completed it provides statistics of the model, i.e. over the estimated values [29]

Step 5: Measures

The next step includes identifying measures to each risks. Identifying measures to risks considered in need for it was not covered within the FAIR-method. This step is therefore based on how Secure State currently identified alterations combined with how FAIR estimates the risk initially. These measures are identified by making the participants individually write down measures to the risks considered in need of mitigation. For each measure the risk ID, to which risk the measure tend to decrease, shall be clear. Additionally, it shall be clear whether the measures aim to decrease the LEF, i.e. prevent the risk, or decrease the LM, i.e. reduce the risk. A new estimation of either the LEF or LM is performed given that the identified measure would be implemented. A new estimation of LEF is performed if the measure prevents the risk and a new estimation of LM is performed if the measure aims to reduce the consequence of the risk. Table 4.7 presents a view of performing and documenting a new estimation when the measure aims to prevent the risk. Table 4.8 presents a view of performing and documenting a new estimation when the measure aims to reduce the consequence of a risk.

Table 4.7: *A example determining a new LEF based on an identified measure.*

Risk ID	**Measure ID**	**Measure Type**	**Minimum value**	**Maximum value**	**Most likely value**
1.1	M1	Prevent	0,5	1	0,7
1.2	M2	Prevent	0,1	1	0,5

Table 4.8: *An example determining a new LM based on an identified measure.*

Risk ID	**Measure ID**	**Measure Type**	**Minimum value**	**Maximum value**	**Most likely value**
1.3	M3	Prevent	4h*$100	30h*$100	8h*$100
2	M4	Prevent	2h*$100	6h*$100	4h*$100

Step 6: Risk assessment given an implemented measure

The new value for LEF and LM, which representing the probability and consequence after the identified measure is implemented, is used as input to the Monte Carlo method. The Monte Carlo method generating 1000 new simulations which are placed in the "heat map" once again.

4.4 Evaluation of method

The responses from the questionnaire, given by the participants of the risk analysis where the proposed quantitative risk analysis method was used, are presented in Table 4.9. Each column represents a respondent and the rows presenting the grading for each claim.
The claims in the questionnaire are presented in Section 3.4.

Table 4.9: *Responses from the respondents.*

Respondent Claim	**1**	**2**	**3**	**4**
1	4	5	3	5
2	1	1	1	2
3	5	5	3	4
4	3	3	3	4
5	5	3	4	3
6	1	1	4	1
7	5	4	3	5
8	2	3	4	2
9	4	5	4	4
10	3	3	1	3

The results during this part is mostly based on the value each participant gave respective claim. Still, a discussion regarding the quantitative risk analysis tested during the assessment was performed after the assessment. Since the discussion was performed after the questionnaire it made the participants focus mostly on subjects regarding the questions in the questionnaire. Having the questionnaire performed before the discussion made the answers in the questionnaire not be dependent on group pressure.

By estimating a minimum and a maximum value for a risk's LEF and LM, and further include a method called calibration (see Section 2.8), the "correct value" was likely to be covered according to the participants. Additionally, according to the respondents of the questionnaire, dividing risks into smaller components made it easier to find useful information in order to understand and estimate the risk in a sufficient manner. Furthermore, the decomposition was not considered to be complex and arbitrary, instead respondents considered the decomposition to increase the commitment within the assessment group. They considered that the decomposition helped the participants to interpret the risks in the same way. The results of the questionnaire furthermore indicated that the respondent thought that the evaluation of the risks was based on both statistics and human thoughts, however slightly more on human thoughts.

Respondents considered it to be advantageous to include Monte Carlo simulations for the estimation of risks. Additionally, the usage of PERT (i.e. distribute the input over a range including a minimum value, a maximum value, and a most likely value) was considered as an improvement in comparison to how Secure State currently estimates risks. The respondents considered that the result became less arbitrary when risks were estimated over a distributed range. Since the decisions became more thoughtful and understandable compared to only estimating a risk through a pre-defined scale.

Decisions of risk's significance were considered to be discussed within the group. Having discussions regarding risk's significance resulted in a common decision where all inputs made by the participants where taken in to consideration. All participants felt that they were able to contribute, and the decisions reflected opinions of the whole group. There were no tendencies of having a participant dominating the assessment. The participants often felt

that it was complex to estimate the risks further down in the "decision pyramid" (see Figure 4.4) than estimate:

- LEF
- LM

The participants considered it to be unnecessary and complex to estimate LEF and LM by estimating TEF and Vuln, respective primary and secondary losses.
During the risk analysis where the proposed quantitative risk analysis method was tested, participants used the information provided by the decomposition in order to estimate the risks. According to the participants, if different interpretations were identified during the composition of risks, the risks were described as different risk scenarios, which made the risk analysis both more comprehensive and more understandable according to the participants.

The process of decomposing risks into components and divide risks into several risk scenarios increased the time required for the risk analysis. The increased time of the risk analysis can be referred to as making the risk analysis less practical. However, the participants did not considered that the decomposition resulted in unnecessary work, instead respondents considered the decomposition to increase the commitment within the assessment group. The commitment was increased since the task became more understandable. When the task became more understanding the participants felt that they more easily could contribute with their knowledge.

The amount of statistics used for estimation of risks during the risk analysis (where the quantitative method was used) was considered to be different among the participants. Despite this, the result of the questionnaire indicates that the participants thought that the estimations of the risks were based on both statistics and human thoughts. Two of the respondents commonly participated during risk analysis performed by Secure State. These two respondents considered the assessment to include a higher grade of statistics than the other two respondents. Among the two respondents that gave the lowest score regarding the usage of statistics, one had never participated in any risk analysis performed by Secure State before. The other respondent, of the two giving the lowest score regarding the usage of statistics, had been present during a few risk analysis before.

As with SUS, the results of respondent's grading for the claims are converted (see Section 3.4). Table 4.10 presents the converted values of the results from the questionnaire. Each column represents a respondent and the rows present the converted value of the respondent's answer for each claim.

The maximum score for each respondent is 40, this since the answers of the respondents has been interpreted as with SUS, see Section 3.4. As the results in Table 4.10 presents, all respondents had a higher score than the average. The possible values for each response is a value between 0-4 (after the conversion as with SUS) the average score of the ten claims is therefore a value of 20. The final sum of the questionnaire presents that one respondent scored a quite significantly lower value than the other three respondents. Figure 4.7, 4.8, and 4.9 presents a graphical view of the results given by each respondent to each question (before the values were converted). As Figure 4.9 presents, respondent number three (who had the lowest result among the respondents) gave the negative angled questions number six and eight a higher rank (i.e. a worse rank) than all other respondents. Question number six was estimated significantly worse by respondent number three than by the other respondents. Question number six regarded decomposing the risk into smaller components where the claim stated that the process resulted in unnecessary work and less participation within the assessment group. Question number eight regarding if the PERT-analysis was considered hard to apply.

Table 4.10: *Converted responses from the respondents*

Respondent Claim	**1**	**2**	**3**	**4**
1	3	4	2	4
2	4	4	4	3
3	4	4	2	3
4	2	2	2	1
5	4	2	3	2
6	4	4	1	4
7	4	3	2	4
8	3	2	1	3
9	3	4	3	3
10	2	2	4	2
sum	33	31	24	29

Respondent number one scored the highest value. When looking in Figure 4.8 it shows that the person tended to weight the positive angled questions higher compared to the other respondents, and therefore scored a higher score. If looking in to Figure 4.9 it shows that there is not a significant difference between respondent number one's results of negative angled claims compared to the other respondents (except respondent number three, who considered these negative claims be more correct).

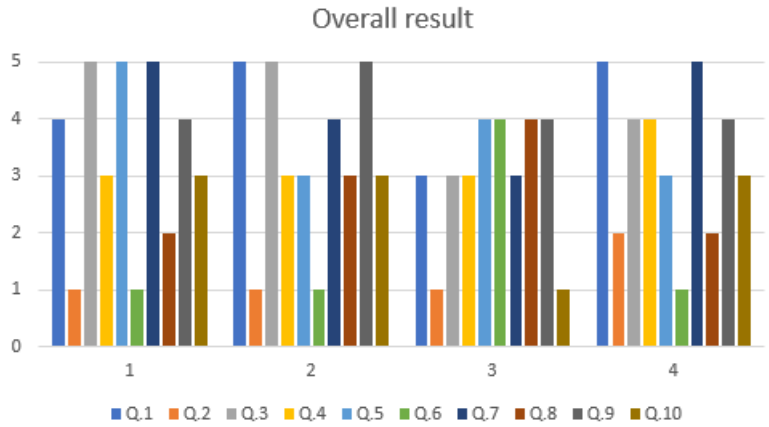

Figure 4.7: *The overall result of the questionnaire.*

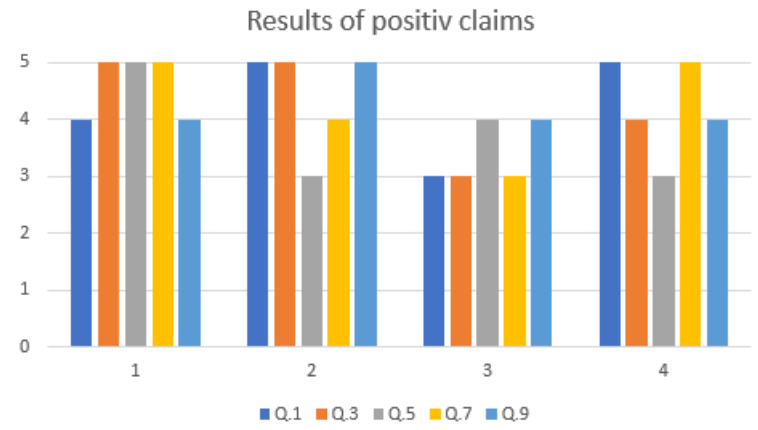

Figure 4.8: *The results of the positive claims from the questionnaire.*

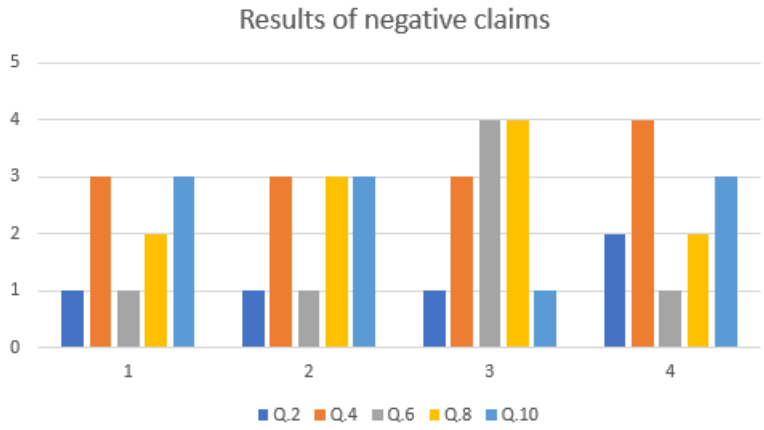

Figure 4.9: *The results of the negative claims from the questionnaire.*

5 Discussion

This chapter aims to provide a discussion where Section 5.1 discusses the results gathered during the process described in Chapter 4 and Section 5.2 provides a discussion regarding the method used for performing this thesis (see Chapter 3).

5.1 Results

Secure State often encounters problems regarding the wrong participants during risk analysis. Therefore, it is important that Secure State clearly provide clients with information regarding the importance of identifying the aim of the risk analysis and what parts of the organization the analysis aims to include in order for the analysis to include required participants. This since the proposed quantitative method also is sensitive towards not including the required participants with enough authority to make decisions in the risk assessment [9]. If necessary participants are not added into the assessment the process of dividing and analyzing risks deeply will become superfluous, and making the strength of the FAIR-inspired method be useless. Therefore, it is important that clients of Secure State know their responsibility of including participants possessing the information necessary in order to gather accurate and precise results [9]. If the clients initially do not include participants to cover included parts of the organization based on the initial scope, either the scope of the FAIR-inspired risk analysis needs to be decreased to be adapted to the situation or the required people needs to be added into the assessment. If the clients can not provide sufficient resources, the resources they do provide (e.g. time and money) will be spent in vain. It is challenging making the clients understand the importance of performing the risk analysis since the clients often see the risk analysis as superfluous and want to spend minimum resources on conducting the assessments. According to Secure State, in scenarios where the client has the one who ordered the risk analysis participating during the assessment it becomes easier encourage the rest of the participants. If the analysis is ordered from someone in the Board of Directors for instance, who are not participating during the assessment it becomes much harder both to encourage the once participating as well as making sure that the client provides the required expertise. Based on this information, Secure State should encourage one of the persons taking the initiative for performing the risk analysis from the client to participate and further collect the people required for the assessment.

Additionally, Secure State wished to base decisions on statistics rather than assumptions. The current method used by Secure State could theoretical include statistics to base decisions upon. One reason identified to way statistics barely was used was the fact that risks identified during the assessments may not have been materialized in the organization before. If the risks are not analyzed more deeply and the participants do not assesses what a risk consists of and targets etc, it becomes hard to use statistics properly. A process of analyzing the identified risks to gather more and deeper information regarding the risks was not included in the current risk analysis method used by Secure State. The approach of estimating identified risks within the selected quantitative method is based on decomposing the risks into smaller components. The aim of decomposing risks into smaller components is to increase the understandings of what each risk consists of and targets [9]. Addressing what the risks consists of and targets increases the possibility of identifying similar risks, yet not identical, which the organization (or similar organizations) has been exposed to before. Furthermore, it enables to identify how vulnerable the organization was towards these similar risks at that time. Therefore, decomposing the risks into smaller components enables to more easily include valuable data based on statistics, which increases the possibility of making the results of the risk analysis reflect the probable future [9].

In order to properly include and use statistical information within the FAIR-approach, statistical information actively needs to be collected. Applying the FAIR-approach and decompose the risk dose not implies that statistical information is used. Instead FAIR provides a framework for structurally using statistical information. The amount of statics used during the quantitative risk analysis according to the participants differed. Since the respondents who commonly participated during risk analysis performed by Secure State considered the possibility of using statistics to be improved, the result indicated that an improvement regarding the possibility of utilizing statistics during risk analysis was achieved. However, the process of including statistical data requires to actively address the statistical information. Accessing statistical information properly requires having the right contacts and accesses within the organization. During the assessment, where the quantitative risk analysis was held, participants were positively set to including statistics from the beginning. They were aware of the fact that including statistical data would increase the time of the analysis, yet willing to try. During the risk analysis there were several occasions were either statistics were not available or the participants did not know were to find the information. If the assessment group would be negative set to including processes to identify statistical data from start (e.g. not willing to increase the time, participants, or putting the extra effort to find the information) it will be hard to encourage the participants to apply statistical data even if the FAIR-inspired method provides tools for it.

The accuracy within the results of the current methodology performed by Secure State was often a matter of what assumptions were being made and how rigorous the thinking which underlying the analysis was [13]. Since the definitions of each level of the scales were not taken into consideration during estimations of risks, the underlying thinking was inadequate. Not having the definitions of each level of the scales taken into consideration during estimations of risks further decreased the possibility of utilizing the available information about a risk properly. Since interpretations of the risk's estimation scales were made independently of its definition during risk analysis performed by Secure State, these scales would most likely be interpreted differently in another time. Not consider or identify proper information to why a risk's probability or consequence should be of a certain value, this value would most likely be estimated differently in another time as well. The risk value is likely to be estimated differently since the participants did not reflect upon why, for example the probability, was estimated to a specific value. This makes the results from Secure State's currently performed risk analysis method non defensible.

Additionally, not consider the actually meaning of each grade in the scale made each participants interpret each grade individually, hence individual assumptions were being taken. Furthermore the meaning of a risk was rarely stated more than briefly mentioned. Interpret risks and the estimations differently among participants makes the results of the analysis responding to different things depending on the participant. Therefore, the process of identifying alterations to either mitigate or reduce the risks ended up in confusing discussions. Since the participants interpreted risks differently, different types of proposals for alterations were mentioned. An alteration suitable for one interpretation of the risk might be questioned from participants who interpreted the risk differently. Using the proposed FAIR-inspired method to decompose the risks into smaller components to make risks commonly interpreted and divide the risks into several risk-scenarios when necessary, can be seen as time-consuming. However, by including these processes, unnecessary discussions based on aberrations could be decreased during the risk analysis. Decrease misunderstandings by putting extra time on dividing and splitting risks can therefor decrease the total amount of time necessary for the risk analysis.

When the time is increased by decomposing the risk and use calibration for each value being estimated a conflict between proactivity and accuracy might be created since the accuracy might increases but the proactivity might decreases by including these processes. Positively, the statistical information gathered, and the decomposition and calibration performed can often be reused during an assessment. This makes the resources required decrease as the assessment progresses. Increasing the initial time required for an assessment might be critical for Secure State since they already experiences that participants in risk analysis do not have commitment and motivation for the task, and therefor might not be willing to increase the effort spent during a risk analysis. However, participants might feel the unwillingness of spending time on risk assessments based on their ignorance of the task and arbitrariness in the process of estimating risks. Therefore, the process of decomposing the risks to properly understand the risks and further structurally identify information in order to use statistical data to make the process less arbitrary, might encourage people to participate. There are researches performed about task commitment which shows the importance of understanding the assignment and feeling able to contribute with valuable information in order to become more involved in the assessment [25]. One can also discuss whether including parts that the clients might not be familiar with before, such as Monte Carlo simulations, could make the client feel left out and therefore decrease the motivation. However, in the currently performed risk analysis method Secure State already does a lot of work related to the task without direct interaction with the client. This has not been raised as an issue yet, and therefor one can argue it will not affect the motivation. Additionally, the aim of hiring consultant is to outsource tasks which are not connected to the core business of the enterprise. Therefore, it is rather an expectation that the work is performed without require the client to be involved at all time.

In order for the risk analysis method to achieve results that can be considered good, i.e. fulfill the required level of accuracy and precision, the performance requires comprehensive resources, including time. The requirement of comprehensive resources will decrease the possibility of a risk analysis to be fully practical. For clients how are not willing to spend sufficient resources on the risk analysis, and only wishes a basic overview of risks connected to the scope, the FAIR-inspired method would still be a good alternative. The process of the FAIR-inspired method requiring most time is gather statistical data. Excluding the process of gathering statistical data therefore decreases the time as well as the need of using different devices, systems, human knowledge, etc, for collecting the statistical data. However, use the knowledge and experience among the participants in a proper way, i.e. include the processes of gather a common understanding of the risks and the estimations will increase the quality of the result in relation to the currently used method which do not include statistical data either [9].

Regardless of the amount of available statistical information connected to a risk, all risks were estimated equally detailed (or non-detailed) within the current risk analysis method. Therefore, when information was available it was often not properly used and when the information was inadequate, the estimations were not adapted and therefore might not manged according to the reality. In the proposed quantitative method the estimations of the identified risks were performed by give the risk a minimum value, a maximum value, and a most likely value. The FAIR-inspired method therefore enabled to be precise when comprehensive information was present, i.e. decrease the range between the estimated minimum and maximum value. When information available was insufficient, the precision could be decreased, i.e. extend the range between the estimated minimum and maximum value. The approach of adapting the precision dependent on the available information enables to achieve accuracy within the result [9]. The possibility of adapting the range to the specific situation in order to achieve accuracy within the result makes the risk analysis method useful. Additionally, achieve accuracy within the results enable the results to be defensible.

As described above, adjusting the estimations dependent on available information are not possible within the current risk analysis method used by Secure State. Consider the possibility of adjusting the assessment of risks based on available information was something which the respondents considered advantageously. They considered it to be advantageous since the ability of estimating risks properly varied a lot. Based on how well the respondents were familiar with the risk, their ability of identifying valuable information connected to the risk and further estimating the risks differed. Ranges of a risk's LEF and LM were in some scenarios during the risk analysis required to be estimated broadly due to the possibility of ending up with a value near the limits. In situations where the ranges of a risk's LEF and LM were required to be set broadly, the participants felt that the process of including a most likely value increased the possibility of gain precision in the estimated rang without decreasing the accuracy. When there was no value considered most likely to occur, the ranges were weighted naturally by setting the most likely value to the average of the range [23]. During the risk analysis where the quantitative method was tested, the participants did often used the most likely value to weight the estimations, especially when estimated a risk's LM. The participants often considered values near the lowest value most advantageously. Still, they did not wanted to exclude a LM of a higher value since if the outcome of the threat would become "unlucky" a high LM would be a realistic value.

Evaluation based on the respondents

Initially, worth mentioning is the fact that participants of the risk assessment, where the quantitative risk analysis was tested, overall were positive towards the proposed quantitative risk analysis method. Most of the reactions during the risk analysis as well as their answers in the questionnaire showed that they considered the method to include improved parts. All the participants worked as information security consultants at Secure State. Regardless of their knowledge in risk analysis specific, they had good knowledge regarding information security in general. Having knowledge in information security provided the participants with a good understanding of the importance of performing risk analysis. Since they worked as consultants in the field of information security they considered it to be important spending time on work related to information security. Therefore, they might represented a group having more positive attitudes compared to the general clients of Secure State towards spending resources on risk analysis. Additionally, be aware of possible improvements by implementing the quantitative method the motivation for using the proposed risk analysis method was probably increased compared to clients who do not have a proper understanding of the opportunities provided by the quantitative method.

As presented in Section 4.4 all participants scored a quite high result. However, one of the participants had a bit lower score compared to the rest. One reason to why that participant scored a lower score might be connected to inexperience. The person who had the lowest score had never participated during a risk analysis before, therefore did not exactly know what to expect. Risk analysis is complex, time-consuming, knowledge demanding, etc. Since the three other participants had other occasions to compare the assessment against, there score indicates that an improvement has been achieved. Worth remembering is that clients of Secure State often include persons who not have earlier experience, therefore the method needs to be appealing to inexperience participants. Question number six regarded decomposing the risks into smaller components, where respondent number three considered the process result in unnecessary work and less participation within the assessment group, see Figure 4.9. Decomposing the risks into smaller components was one, if not the most essential process within the proposed quantitative method. If the clients not having earlier experience within risk analysis, would share the impression of respondent number three, it will be necessary to identify processes to encourage inexperienced participants to decompose the risks. There was no claim scored a bad result among the positive angled claims, see Figure 4.8. However, the result for question number five was the claim among the positive angled ones that was given the lowest score in total. Question number five regarded the usage of Monte Carlo. If the respondents were not familiar with the meaning of Monte Carlo, they might not understand why to apply it. There were not a deep explanation to why Monte Carlo could give increased quality within the results prior to the questionnaire or assessment, which might reflected upon the result. However, the usage of Monte Carlo is not something that affects the work of the clients during the assessment. The Monte Carlo simulations would be performed by Secure State after the risk assessment workshop is performed. Therefore, having the clients understand the process deeply is not necessary.

5.2 Method

The method of the thesis mostly consisted of a qualitative approach, i.e. was based on subjective inputs, gathered by a combination of several data collection methods. Collecting data regarding Secure State's current risk analysis method and its performance through several data collecting methods favoured the quality of the study. The quality of the study, when applying several methods for gathering data, was increased since a deeper understanding of the subject examined was gained [16]. Additionally, the usage of several methods for gathering data had a positive impact on the credibility of the study. The credibility increased since the result included fewer influences from the author's own expectations and preconceptions [20, 38].

This study managed both information collected by the investigator herself, as well as information already existed and collected by other investigators. Information collected by other investigators, might has been collected for an other purpose than the purpose of this study or being angled. This is important to consider in order to gather valuable and appropriate information from theoretical sources. Using information collected by both the author herself, and by other investigators enabled to combine the findings into beneficial outcomes [16].

Using three methods for gather information regarding how Secure State performs risk analysis and its accompanying problems, i.e. interviews, observations, and document reviews, enabled to collect different kind of data within different scenarios. An advantage of using observation compared to interviews was that results from the observations was not as vulnerable towards persons unwillingness of answer or discuss sensitive questions [27]. However, the results from the interview performed included deeper information regarding

problems within the risk analysis method currently used by Secure State. The interview was held on a person having high expertise within the current risk analysis method performed by Secure State. The respondent desired to improve their way of performing risk analysis by including quantitative measures. Since the respondent desired to improve Secure State's risk analysis method, the interview became less sensitive towards unwillingness of discussing their problems, i.e. respond to sensitive questions.

One limitation of gathering data regarding Secure State's current way of performing risk analysis was that only one interview was held. Only performing one interview made the information gathered through interviews only depend on one person's thoughts. However, the respondent was an expert within the subject and further in charge of the risk analysis performed by Secure State. Therefore, the respondent had both a wide and deep knowledge regarding their risk analysis method, making the answers contain valuable information. The respondent was present during almost all risk analysis performed by Secure State. The semi structured approach for the interview enabled to adapt the pre-defined questions (presented in Section 3.2) during the interview to extract comprehensive information [20]. Furthermore, the interview was held at Secure State's head office, a natural place for the respondent, enabling avoiding artificial responses [16].

There were two observation performed during this study. The aim of the two observations was to examine two different occasions where Secure State performed risk analysis at their clients. The scope of the two risk analysis and the participants present were different during the two occasions. The sources from where data was gathered were therefore different. Using different sources for gathering results increased the credibility of the information gathered during the observations [38].

Implementation of method

The result, i.e. the fulfillment of criteria, from each risk analysis method examined was quite even and furthermore the fulfillment was fairly high (see Table 4.3). Two reason identified, to why the result of the examined quantitative risk analysis was both of a high fulfillment and even, were:

- Only methods considered worth investigating were examined, and therefor tended to fulfill several of the criteria. Methods which did not seem appropriate were scoped out in an earlier stage of this study, and therefore not included in the evaluation of their fulfillment.
- The criteria were not that specific, making a lot of methods fit in to the criteria.

A deeper investigation of the methods' fulfillment of each criterion and a second iteration of the selection of method would have enabled identifying more critical criteria, as well as a deeper investigate regarding how much each method fulfilled each criterion. This would further have increased the quality of the selection of method. However the limitation regarding time and money for the investigation of methods did not enabled further investigations. As described in Section 3.3 some criteria were considered required to be fulfilled. A criterion seen as required but still not affected the accuracy or precision within the result of a risk analysis method was enough available information. The criterion enough available information concerned the information identified for the quantitative risk analysis methods. This criterion did not necessarily sow away methods that was inappropriate. However, if the information available was not enough in order to apply the method in a sufficient way, the result of the risk analysis would be negatively affected. Based on that, sufficient available information became a required criterion. Information might would have been possible to gather towards the methods that did not fulfilled the criterion. However, the time set for the literature review

was narrow, making it impossible spending a huge amount of time on finding specific information. In some cases money was required to spend in order to gather further information. Firstly, one of the required criterion demanded that the selected quantitative risk analysis method was open source, i.e. was possible to be performed without paying a fee. Secondly, if a sum was required to be spent in order to buy a book to collect the information needed, exceptions were taken. However, the available information identified regarding methods was commonly to inadequate in order for it to be profitable buying further information. The criterion of accessing enough information about the methods was often not fulfilled. If the time limit for gathering data about different methods would be increased, more methods would probably have fulfilled that criterion. Gathering more data regarding all methods would further have increased the quality of the whole process of selecting a method. Having more information about the different risk analysis methods would have enabled to evaluate how much (or little) methods fulfilled each criterion. For the process of selecting a risk analysis method during this thesis, the result did not became to much negatively affected by the limited amount of time for gathering information of different risk analysis methods. This since the FAIR-approach did provided sufficient information as well as fulfilled most of the criteria.

Additionally, further investigation within risk analysis methods would have enabled identify pros and cons in each method. These findings could then have been possible to combined to create an adopted version of several methods. The selected method was as presented earlier in some extent adapted to fit some processes within Secure State's current way of performing risk analysis. This in order to reuse positive parts of the framework which has been developed within the company. On the other hand it might be preferable not changing to much within the selected method. Having processes changed, which has been developed for a specific reason might decrease the quality of the result, if not extensive researches is performed. After the FAIR-method was selected, the processes of including the Monte Carlo simulations and PERT distribution initially was aimed to be evaluated to see whether there were other alternatives more suitable. However, the FAIR approach had recently upgraded their version where a Bayesian network earlier was used to include a probability factor within the result. Bayesian network is a graphical model for managing the probability in non-deterministic variables [24]. After the updated version of the FAIR-method, the Bayesian network was replaced by Monte Carlo simulations. According to FAIR, this upgrade improved the results of the FAIR-method [9]. Convict that there is an other process more suitable to include in order to managed non-deterministic variables than Monte-Carlo would therefore require researches where sufficient resources would have to be spent.

Evaluation of the study

In order to evaluate the selected quantitative risk analysis method, the risk analysis method selected was used during a risk analysis. Additionally, participants answered a questionnaire regarding their thoughts of the selected quantitative risk analysis method, in terms of performance and gathered results. The structure of the questionnaire was inspired by the SUS approach [35]. However, the claims that were asked the respondents were adapted in order to fit this specific evaluation. There are several studies present regarding how evaluations can gain credibility by using SUS [35]. However, the findings differed among the investigations. An example is the number of respondents which are required to participate in the questionnaire. The number of participants required, in order to obtain credibility within the results of a SUS evaluation, are different dependent on the investigator. Some investigators advocates that at least 50 participants needs to respond to the questionnaire in order to provide credibility within the result. Others advocate that there only requires two persons in order to gain valuable results [35]. Since the evaluation did not use similar claims as those provided by SUS, the interpretations of the results can not follow the structure as presented in SUS. However, the fact that a higher number of respondents of the questionnaire, given

that they participated during a risk analysis where the proposed quantitative method was used, would have increased the credibility of the results from the questionnaire. Additionally, as mentioned earlier the respondents who tested the risk analysis method had deep knowledge within the area of information security, making them understand the need of a well structured method. Since the respondents were employees at Secure State who ordered the thesis in order to improve there risk analysis method, the respondents are probably more positive for increasing objectives input based on statistic than the average of Secure State's clients. On the other hand, they might had a lot of expectations hard to meet and therefore one can advocates that for those who do not have as high expectations the method would have been evaluated to be even better.

Furthermore, the adapted SUS approach uses subjective inputs for the evaluation of the presented risk analysis method. The evaluation regarding the results from the selected quantitative risk analysis method does not consider any measurement of improvements. Including a quantitative tool within the evaluation of the selected risk analysis method would further have increased the credibility in the results of the evaluation [13]. However, a quantitative evaluation would require extensive resources, e.g. information, time, and tools. Therefore, it was impossible to use a quantitative tool for evaluate the selected risk analysis method during this thesis. Additionally, having the method tested several times considering different scope and participants would also have increased the reliability of the result. Again, based on time and possibility of participate during risk analysis this was not possible either.

5.3 The work in a wider context

Societal aspects

Set to today's society, information security is a subject that needs to be taken into consideration. The evaluation of information technology (IT) has moved fast and created huge possibilities world wide. Organizations are today dependent on their implemented IT systems in order to be operative. The functionality within the systems become more complex each day passing by. However, aligned with the usage of complex IT systems, vulnerabilities arises. Within today's society, organizations are constantly being exposed to attacks with the aim of harm the organizations availability, integrity, or confidentiality. Protect themselves from exposure is therefore necessary. Additionally, in order to protect something, it requires to know what to protect and what the organization is exposed to, hence performing risk analysis is necessary in the initial work of protect the organization [26, 37].

Ethical aspects

Performing risk analysis is a sensitive subject. It is a result of what the organization fear the most. The result of a risk analysis contains information regarding possible risks toward the organization, the risk's probability to occur, as well as their impact. Furthermore, the result of a risk analysis indicates what actions that need to be taken in order to mitigate risks, and which risks that are considered accepted [9, 13, 33]. Given this knowledge, attacker enables to increase the efficiency of their attacks, hence if the knowledge reaches the wrong hands tremendous consequences can be the result. Therefore, the results of a risk analysis contain confidential information which must be managed with high caution in order to not be exposed.

6 Conclusion

A lot of criticisms has been raised against qualitative approaches for assessing risks, therefore this study aimed to investigate the current qualitative risk analysis method performed by Secure State. During the investigation, problems regarding qualitative risk analysis were identified together with accompanying affects on the result of a risk analysis. In order to resolve these identified problems, a quantitative risk analysis method was developed for Secure State. Initially, three research question were established with the aim of being addressed by the results of this study. The following chapter will discuss findings regarding each research question.

Which pros and cons exists in the current risk analyses methodology performed by Secure State?

In the risk analysis, currently used by Secure State, risks were estimated based on its probability to occur and accompanying consequences. These two factors, probability and consequence, were determined based on an ordinal scale between one and four. The estimations performed by client's of Secure State were rarely considered carefully. Instead, the estimations of each risk were briefly discussed, where the participant having the strongest thoughts, ended up determining the risk value. Additionally, the ordinal scale used within the current method of Secure State was interpreted differently by different participants. Each level of the scale did include a definition, however the definition was barely not used during the assessments. Individual interpretations made the estimations of risks arbitrary. Furthermore individual interpretations of risks were made since the process of defining what a risk consisted of as well as targeted was inadequate. Based on not defining the mean of the risks, confusing discussions regarding proper alterations to mitigate risks were commonly occurring. Not really understand the assignment and what the estimations actually was referred to did not have a positive impact on the already negative attitude of participants.

Furthermore, Secure State often encounters problems regarding the wrong participants. Therefore, inputs become inadequate and affected the result of the risk analysis negatively. This negative affection on the results made the prioritization of which risks seen as the most critical biased. The prioritization became biased since it was not created based on the entire organization. Important risks to parts of the organization not having a represen-

tative present during the risk analysis, were easily missed or estimated in a defective manner.

There were also positive parts identified in the process of how Secure State performs risk analysis. These parts were reflected in the criteria where each risk analysis method was evaluated through. Secure States method included a structure way of identify alterations, and also followed up regarding their possibilities to decrease either the probability or consequence of a risk. Also the way of individually identify risks and alteration was reused and included in the FAIR framework. This enabled everyone to actually raise there experience based on their expertise. Also having human expertise utilized and this by performing workshops was also positive and included in the presented method. Since there will be hard finding statistics on everything it will be a good complementary to include human experience and expertise.

How can the result be improved by including quantitative measurements during a risk analysis. How should a quantitative approach be used when performing risk analyses at Secure State?

The usage of a stochastic modelling tool like Monte Carlo method can bring legitimacy to a risk analysis and make the result become more defensible. As presented earlier, risk analysis requires to use imperfect data because the information concerns the future, i.e. the uncertain. However, the usage of PERT and Monte Carlo method increase the value of the imperfect data. Applying a PERT distribution and further use the Monte Carlo method during risk analysis, which are inherently designed to deal with the uncertainty in data, increased the credibility within the result. Additionally, using the process of decompose the risks into smaller components increases the possibility of identifying statistics proper to base the estimations upon. Using statistics within the estimations increases the possibility of making the results of the risk analysis reflect the probable future based on actual data rather than assumptions.

How can different key components from both qualitative and quantitative risk analysis methods be combined in order to make Secure State extracted improved results from their risk analysis?

The selected quantitative risk analysis method included decomposing a complex subject into clearer, more readily analyzed components. Having the risk decomposed increased the understanding towards the risk. When the understanding increased, reasoned judgments about the risk were applied. Manage the data in a sufficient way (i.e. decompose the risk) enabled to identify the data needed. To further apply a method inherently designed to deal with the uncertainty in data, accuracy and precision within the results becomes increased.

By estimating a minimum and a maximum value for a risk's LEF and LM, and further include a method called calibration (see Section 2.8), the estimated "correct value" was likely to be covered. Since calibration (see Section 2.8) was applied during the risk assessment process, participants ended up with ranges which they were 90% confidence in.

The quantitative risk analysis method proposed and further used for a risk analysis performed at Secure State enabled to be precisely when comprehensive information was present, i.e. decrease the range between the minimum and maximum value. When information available was insufficient, the precision was decreased, i.e. the range was extended. The approach of adapting the precision dependent on the available information, enabled to achieve accuracy within the result. The possibility of adapting the range to the specific situation in order to achieve accuracy in the result makes the risk analysis method useful. Additionally, maintenance of accuracy within the result making the defensible.

Bibliography

[1] COBRA Risk Security Analysis. *COBRA Risk Consultant*. 2003, Accessed 2017-04-01. URL: http://www.security-risk-analysis.com/riskcon.htm.

[2] James B. Anderson. *Quantum Monte Carlo. [Electronic resource] : origins, development, applications.* New York : Oxford University Press, 2006., 2006. ISBN: 9780195310108.

[3] Terje Aven. *Fondations of Risk Analysis*. Second edition. University of Stavanger, Norway, 2012. ISBN: 978-1-119-96697-5.

[4] Linköpings universitets bibliotek. *UniSearch*. Accessed 2017-02-02. URL: https://www.bibl.liu.se/soka/unisearch?l=sv.

[5] Alan Calder and Steve Watkins. *IT governance : an international guide to data security and ISO27001/ISO27002. [Elektronisk resurs].* London, United Kingdom : Kogan Page Limited, 2015., 2015. ISBN: 9780749474065.

[6] G. (1) Cao, Y. (1) Duan, S. (1) Minocha, and T. (2) Cadden. "Systemic capabilities: the source of IT business value." In: *Information Technology and People* 29.3 (2016), pp. 556–579. ISSN: 09593845.

[7] Richard A. Caralli, James F. Stevens, Lisa R. Young, and William R. Wilson. "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process." In: (2007).

[8] Backlund F. and Hannu J. "Can we make maintenance decisions on risk analysis results?." In: *Journal of Quality in Maintenance Engineering* 1 (2002), p. 77. ISSN: 1355-2511.

[9] Jack Freund and Jack Jones. *Measuring and Managing Information Risk*. A FAIR Approach. Butterworth-Heinemann, Elsevier., 2015. ISBN: 978-0-12-420231-3.

[10] Barbara Gładysz. "Fuzzy-probabilistic PERT." In: *Annals of Operations Research* 258.2 (2017), pp. 437–452. ISSN: 02545330.

[11] Rosemary J. Harris. "Random walkers with extreme value memory: modelling the peak-end rule." In: (2015).

[12] Douglas W. Hubbard. *How to measure anything. [Electronic resource] : finding the value of "intangibles" in business, third edition.* Hoboken, N.J. : John Wiley & Sons, c2014, 2014. ISBN: 9781118539279.

[13] Douglas W. Hubbard. *The failure of risk management. [Electronic resource] : why it's broken and how to fix it.* Hoboken, N.J. : John Wiley & Sons, c2009, 2009. ISBN: 9780470387955.

[14] *Implementing the NIST : cybersecurity framework. [Elektronisk resurs].* Rolling Meadows, Ill. : ISACA, [2014], 2014. ISBN: 9781604203578.

[15] Investopedia. *Tangible Asset*. 2017, Accessed 2017-06-10. URL: http://www.investopedia.com/terms/t/tangibleasset.asp.

[16] Dag Ingvar Jacobsen, Gunnar Sandin, and Caroline Hellström. *Vad, hur och varför : om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen.* Lund : Studentlitteratur, 2002, 2002. ISBN: 9144040962.

[17] Bilge Karabacaka and Ibrahim Sogukpinar. "ISRAM: information security risk analysis method." In: *Computers & Security* 24.2 (2005), pp. 147–159. ISSN: 01674048.

[18] Yoon Hee Kim, Fabian J. Sting, and Christoph H. Loch. "Top-down, bottom-up, or both? Toward an integrative perspective on operations strategy formation". In: *Journal of Operations Management* 32.7 (2014), pp. 462–474. ISSN: 0272-6963.

[19] Joel Lanz. "Conducting Information Technology Risk Assessments." In: *CPA Journal* 85.5 (2015), pp. 6–9. ISSN: 07328435.

[20] Per Lekvall, Clas Wahlbin, and Per Frankelius. *Information för marknadsföringsbeslut.* Göteborg : IHM Publ., 2001 ; 2001. ISBN: 9186460854.

[21] 2) Leung B. (1 and R.J. (3) Steele. "The value of a datum - how little data do we need for a quantitative risk analysis?." In: *Diversity and Distributions* 19.5-6 (2013), pp. 617–628. ISSN: 13669516.

[22] Meharipedia.org. *Meharipedia*. Accessed 2017-03-15. URL: http://meharipedia.org/mehari-method/.

[23] Microsoft. *Use a PERT analysis to estimate task durations*. 2007, Accessed 2017-04-18. URL: https://support.office.com/en-us/article/Use-a-PERT-analysis-to-estimate-task-durations-864b5389-6ae2-40c6-aacc-0a6c6238e2eb#bm1.

[24] Ankush Mittal and Ashraf Kassim. *Bayesian network technologies. applications and graphical models. [Elektronisk resurs].* Hershey, PA : IGI Pub., c2007, 2007. ISBN: 9781599041414.

[25] Anette Olin. *Skolans mötespraktik - : en studie om skolutveckling genom yrkesverksammas förståelse.* Göteborg studies in educational sciences: 286. Göteborg : Acta Universitatis Gothoburgensis, 2009, 2009. ISBN: 9789173466646.

[26] Alberto Partida and Diego Andina. *IT security management. [Elektronisk resurs].* Lecture notes in electrical engineering: 61. Dordrecht ; London : Springer, c2010., 2010. ISBN: 9789048188826.

[27] Ulf Paulsson and Maria Björklund. "Seminarieboken : att skriva, presentera och opponera. 2. uppl." In: (2012).

[28] Miguel Ramirez de la Huerga, Victor A. Bañuls Silvera, and Murray Turoff. "A CIA–ISM scenario approach for analyzing complex cascading effects in Operational Risk Management." In: *Engineering Applications of Artificial Intelligence* 46.Part B (2015), pp. 289–302. ISSN: 0952-1976.

[29] RiskAMP. *The beta-PERT Distribution*. 2017, Accessed 2017-09-01. URL: https://www.riskamp.com/beta-pert.

[30] Sally Rumsey. *How to find information. [Elektronisk resurs] : a guide for researchers.* Open UP study skills. Maidenhead : McGraw-Hill/Open University Press, c2008, 2008. ISBN: 0335235549.

[31] Antonio Santos Olmo Parra, Luis Enrique Sanchez Crespo, Esther Alvarez, Monica Huerta, and Eduardo Fernandez Medina Paton. "Methodology for Dynamic Analysis and Risk Management on ISO27001." In: *IEEE Latin America Transactions* 14.6 (2016), pp. 2897–2911. ISSN: 15480992.

[32] James Shanteau and Ward Edwards. “Decision making by experts: Influence of five key psychologists.” In: *Neuroeconomics, judgment, and decision making*. Frontiers of cognitive psychology. Psychology Press, 2015, pp. 3–26. ISBN: 978-1-84872-659-8.

[33] Mark Talabis and Martin Jason. *Information Security Risk Assessment Toolkit*. Syngress, 2013. ISBN: 987-1-59749-735-0.

[34] Ding Tan. “Quantitative Risk Analysis Step-By-Step”. In: (2002).

[35] Usability.gov. *System Usability Scale (SUS)*. Accessed 2017-04-28. URL: https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html.

[36] Mihailescu Vladimir Lucian. “Risk analysis and risk management using MEHARI.” In: (2013).

[37] Shelly Ping-Ju Wu, Detmar W. Straub, and Ting-Peng Liang. “How Information Technology Governance Mechanisms and Strategic Alignment Influence Organizational Performance: Insights from a Matched Survey of Business and IT Managers.” In: *MIS quarterly* 39.2 (2015), pp. 497–518. ISSN: 02767783.

[38] Robert K. Yin. *Case study research : design and methods.* Applied social research methods series: 5. London : SAGE, cop. 2009, 2009. ISBN: 9781412960991.