Institutionen för datavetenskap
Department of Computer and Information Science

Examensarbete

Risk analysis review

av

Jacob Bergvall och Louise Svensson

LIU-IDA/LITH-EX-G--15/046--SE

2015-06-12

Linköpings universitet

Linköpings universitet
SE-581 83 Linköping, Sweden

Linköpings universitet
581 83 Linköping

Linköpings universitet
Institutionen för datavetenskap

Examensarbete

Risk analysis review

av

Jacob Bergvall och Louise Svensson

LIU-IDA/LITH-EX-G--15/046--SE

2015-06-12

Handledare: Marcus Bendtsen
Examinator: Nahid Shahmehri

Students in the 5 year Information Technology program complete a semester-long software development project during their sixth semester (third year). The project is completed in mid-sized groups, and the students implement a mobile application intended to be used in a multi-actor setting, currently a search and rescue scenario. In parallel they study several topics relevant to the technical and ethical considerations in the project. The project culminates by demonstrating a working product and a written report documenting the results of the practical development process including requirements elicitation. During the final stage of the semester, students form small groups and specialise in one topic, resulting in a bachelor thesis. The current report represents the results obtained during this specialization work. Hence, the thesis should be viewed as part of a larger body of work required to pass the semester, including the conditions and requirements for a bachelor thesis.

Abstract

The risk analysis process is the foundation of creating secure systems. An accurate and well defined risk analysis will therefore be a big help for any company, indicating what resources are needed and where they should be put to use. It can be difficult to know which risk analysis methodology to use given a set of parameters such as available resources, time, money etc. In this review we will introduce several different risk analysis methodologies and classify them using our risk analysis classification system. Our classification points out some of the pros and cons for each method, making it easier to choose the one best suited for a specific scenario. We will also connect the presented methods with real-world usage of said methods. To do this we have conducted interviews with IT-security experts at several major companies and we will present previous documented usage of risk analysis methods. Larger companies tend to develop their own methods for risk analysis, and smaller companies that do not have enough time or resources to develop their own methods are more likely to use already existing methods. With that said we believe that anyone that works with risk analysis could have use of our review.

Contents

1 Introduction **1**
- 1.1 Motivation . . . 1
- 1.2 Aims . . . 2
- 1.3 Delimitation . . . 2

2 Theory **3**
- 2.1 What is achieved by risk analysis . . . 4
- 2.2 Risk analysis methodologies . . . 5
  - 2.2.1 Attack trees . . . 5
  - 2.2.2 CRAMM . . . 7
  - 2.2.3 ISRAM . . . 10
  - 2.2.4 OCTAVE Allegro . . . 12
  - 2.2.5 COBRA . . . 15
  - 2.2.6 Mehari . . . 17
  - 2.2.7 Magerit . . . 19
  - 2.2.8 CORAS . . . 21

3 Methodology **24**
- 3.1 Classification of risk analysis methods . . . 24
- 3.2 Conducting the interviews . . . 26
- 3.3 Previous documented usage of risk analysis . . . 26

4 Results **27**
- 4.1 Classification of risk analysis methods . . . 27
- 4.2 Interviews with IT-security experts . . . 28
- 4.3 Previous documented usage of risk analysis . . . 30
  - 4.3.1 Attack trees . . . 30
  - 4.3.2 CRAMM . . . 30

5 Discussion **31**
- 5.1 Methodology . . . 31
- 5.2 Results . . . 32
- 5.3 A broader perspective . . . 32

6 Conclusion **33**

7 Appendix A - Interview questions **36**

1 Introduction

Technology today has a big impact on communication, both in the manner of daily usage in our private lives and even more when it comes to business. While this creates possibilities people never could have dreamed of, it also leads to problems regarding vulnerability and accessibility. Have you ever asked yourself, "Should I worry when using my credit card on the Internet?", "How safe is my Internet bank account?", "How many doctors have access to my personal health records?" or "Can I be sure that I am the only one reading my e-mail?" [1]. Due to the big, self-propelled and complex systems that modern technology development has led to, it is very easy to access information and communicate today. Despite the fact that this opens a lot of possibilities it could at the same time be risky. Technology becomes a risk when it is used to control critical components in our surroundings and when people make devastating decisions based on inaccurate data. The concept of risk can be described as a combination of the probability of occurrence of a security breach and the consequences of said security breach. When it comes to companies, important and sometimes secret information is stored in databases and accessed by various communication mediums. The problems regarding vulnerability and accessibility could be major if handled in the wrong way. How can companies handle these problems and still maintain the confidentiality, integrity and availability of their work?

1.1 Motivation

Companies are facing risks on a daily basis, it can be that their system crashes or third parties learns or even changes important information. This might lead to system activities not being able to perform its tasks properly or maintain confidentiality, integrity and availability of the systems data. Threats against companies can be of both human and nonhuman character and can be both intentional and unintentional. A server can crash, which means that the availability no longer is maintained. A hacker can attack the system which could affect both confidentiality and integrity. To be able to protect themselves against all kinds of threats, companies need to be aware of the threats.

It is important to have an insight into the definition of risk itself. This will help significantly when it comes to choosing the best risk analysis methodology for any given situation [1]. And by best, we mean a methodology where the approach and the results fit the company's needs and resources and which kind of threats they need protection from. It requires qualitative insight to evaluate systems from a risk perspective and the first step towards a secure system is to choose a suitable risk analysis method. Many risk analysis methods have been proposed, however there is no one method that suits all situations, and choosing the appropriate method is not always trivial.

1.2 Aims

- The primary aim of this review is to survey scientific literature in order to find proposed methods and to suggest a classification of these methods in order to alleviate the choice of method.
- The secondary aim is to find scientific applications and real world usages of risk analysis methods, and if possible connect these with the classification previously done.

1.3 Delimitation

The field of risk analysis is vast and stretches from mechanical engineering to medical science and IT-systems. It would not be possible to cover all available methods in this review and we have therefore chosen to only focus on risk prevention in IT-systems. Even though we limit the review to the area of IT-systems, there are still hundreds of risk analysis methods to look into and classify. To make the review compact but at the same time thorough enough for future use, we will analyse and classify eight different risk analysis methods. We will also limit ourselves when it comes to performing interviews regarding risk analysis, and only interview IT-experts with extensive knowledge in the field rather than just interviewing any company representative.

2 Theory

"Risk assessment is the foundational skill of all other security skills. It is like basic math to accounting, finance, or science. [1]" The basic risk formula $Risk = consequence \times probability$ illustrates that there are two parts to take into account when calculating risk. The first one, consequence, can have many different forms such as trust, violation of the law, etc. Money is an easy to understand and convenient surrogate for the word consequence. It does not matter if you are a maintenance worker, risk analysis expert or the CEO of a major company. They can all grasp the concept of "if this happens, it will cost us that amount of money". The second part of the equation, probability, illustrates how often specific events will occur. There might be an individual that has your particular system in mind when developing a system attack. Furthermore, this individual might have some inside information from the system which makes the attack harder to fend off. Another possible event is that someone performs a large number of attacks on several systems simultaneously. The fact that the probability of each of these attacks is completely different should not be forgotten while performing the risk analysis. It will often be a waste of resources if you get your probabilities mixed up. For example, if you give a high probability to event A and a low probability to event B, and then realize that in the real world the probabilities are the opposites of that. This means that you have spent a lot of resources to prepare for event A while event B really is more likely to occur [2].

The purpose of risk analysis is to find all possible risks within a system. This is simply impossible due to the fact that risk analyses are performed by humans and no one person has complete insight into every part of a system. Not even a group of risk analysis experts can perform a risk analysis that is 100% accurate. The challenge is to perform the analysis in an organized way so that the result becomes as accurate as possible. An essential part of performing a risk analysis is to know where to limit the analysis. You can not investigate all possible risks at an extremely detailed level. This can lead to the work process being halted completely. This is often referred to as "analysis paralysis" [3]. It means that you are so focused on getting in on every little detail that your over all work progress is at a standstill. Another common type of "analysis paralysis" occurs when you can not quite consider yourself finished with the analysis. You still find these things that need to be taken into account, even though you just spent countless hours finishing the analysis.

There are many different methods for risk analysis and their biggest problem is that they all rely heavily on the people performing the analysis. Therefore, the analysis is only as good as the people performing it. This means that subjective opinions becomes a natural part of the analysis and that other people performing the same analysis may come to other conclusions regarding what the biggest risks are. It is important to note that the area of IT-security is dynamic and constantly evolving, which creates a need for the development of new and improved risk analysis methodologies.

2.1 What is achieved by risk analysis

From a general standpoint, all risk analysis methodologies have two main components:

1. Analyse risks.
2. Recommend countermeasures to mitigate the risks.

The risk analysis process is the foundation of creating secure systems. The countermeasure selection process, staff deployment, the development of policies and procedures, training and emergency preparedness all rely on information from the risk analysis. This tells us that the foundation built by the risk analysis will affect both the owner and the users of the system in many different ways. An accurate and well defined risk analysis will therefore be a big help for any company, indicating what resources are needed and where they should be put to use.

All risk analysis methodologies include the following elements [1]:

- *Asset characterization:* Understand and describe the organization's assets.
- *Threat identification:* Understand and describe what threats there are against the organization's assets.
- *Consequence analysis:* Understand and describe the criticalities of the listed assets to the organization's mission and the consequences to the organization of a successful threat action.
- *Vulnerability analysis:* Understand and express the vulnerabilities of the organization's assets.
- *Threat assessment:* Understand how threat actors view the organization's assets and which assets the threat actors would find most interesting.
- *Risk assessment:* Express risk in the form of a calculation. This should be scalable, so that risk can be calculated for any single asset, or for the entire organization.
- *Risk prioritization:* Prioritize the risks, so that the most important risks can be mitigated first and the least important risks will be mitigated last.
- *Risk management:* Provide recommendations for countermeasures to mitigate the risks.

Different risk analysis methodologies express these attributes in different ways and may use different terminologies to describe them. This will become clear in Sections 3.3 and 5 in this report, where we introduce several different methodologies and classify them using our risk analysis classification system.

2.2 Risk analysis methodologies

In this section we will present different risk analysis methodologies that will later be compared and divided by our risk analysis classification in Section 5. All methods except for one (COBRA) presented in this review can be considered "open-source" due to the fact that their models are free and easy to access. The COBRA methodology is not so much a documented process as a downloadable program, which you have to pay for to get full access to.

2.2.1 Attack trees

"If we can understand all the different ways in which a system can be attacked, we can likely design countermeasures to thwart those attacks. And if we can understand who the attackers are – not to mention their abilities, motivations, and goals – maybe we can install the proper countermeasures to deal with the real threats." [7] Basically, this means that if you want to know how you can protect your system from different attacks, you have to "become the attacker". This is the foundation of the attack tree method, to view risks from the point of the attacker, instead of the defender. This will give an understanding of the systems vulnerabilities and will help to improve its defenses.

Attack trees are models of reality and provide a formal methodical way of describing systems security, based on varying attacks. They are a simplified version of complex real world events. The accuracy with which the underlying events are known depends on different factors including the effort and time spent studying them. The attack tree method represent attacks against a system in a tree structure, with the goal of the attack as the root node and different ways of achieving the goal as leaf nodes. The next step is to treat every new leaf node as if it was the root node and then you add new leaf nodes. This process is then repeated until you do not have any new leaf nodes. As with most risk analysis methodologies it sometimes becomes necessary to make assumptions based entirely on the information at hand. This means that the accuracy of the analysis will be limited by the correctness of the assumptions. To ensure best possible results, the conclusion reached by the attack tree methodology should be compared to the results from other risk analysis methodologies. Another way to improve the accuracy of an attack tree is to let others, preferably security experts, evaluate your tree and think about ways to improve it. This step can in theory be repeated an infinite amount of times, since it is impossible to create the perfect attack tree with 100% accuracy. The people in charge of the risk analysis will therefore be forced to decide when the attack tree is "good enough", to prevent the risk analysis process from consuming too much time and resources. Three conditions must be present in order for an attacker to carry out an attack against a defender's system.

1. The defender must have vulnerabilities or weaknesses in their system.

2. The attacker must have sufficient resources available to exploit the defender's vulnerabilities. This is known as capability.

3. The attacker must believe they will benefit from performing the attack. The expectation of benefit drives motivation.

The responsibility for condition 1 lies completely on the owner of the system, the defender. Whether condition 2 is satisfied depends on both the defender and the attacker. The defender has some influence over which vulnerabilities that exist and what level of resources will be required to exploit them. Different attackers have different capabilities. Condition 3 mostly involves the attacker. It represents the motivation to carry out the attack. The defender may have a role if their actions provoke an attacker to carry out an attack [8].

Figure 1 belongs to B. Schneier [7] and is often used to describe the attack tree method in an intuitive way. The main goal of the attack is to open a safe.

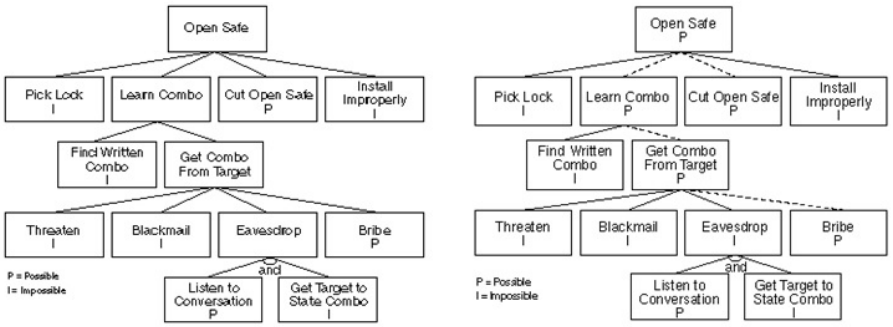

Figure 1: Attack tree, Step 1 and 2

Note that the nodes in Figure 1, step 1 can be divided in AND nodes and OR nodes. In this particular case, all nodes are OR nodes except for "Eavesdrop" which is marked as an AND node. The OR nodes can be viewed as alternatives, an attacker can pick the lock or learn the combination and does not have to do both to achieve the goal. The AND node illustrates that to be able to eavesdrop, an attacker have to both listen to a conversation and get the target to state the combination. Once this basic attack tree structure with AND and OR nodes is complete, it is time to assign values to the various leaf nodes. Which values are selected solely depends on what the owner of the system think is important. Any boolean value can be assigned to the leaf nodes and then propagated up the tree structure in the same manner as "possible" and "impossible" in Figure 1, step 1. A few examples of boolean values are legal versus illegal, special equipment needed versus no special equipment and expensive versus inexpensive.

A major advantage with the attack tree method is that it is easy to tailor the attack tree to an organizations own needs and specifications. The method also provides a perspective on the whole system and on what kind of attacks that are most likely to take place."Security is not a product, it's a process. Attack trees form the basis of understanding that process." [7]

2.2.2 CRAMM

Our description of CRAMM is based on the following references: [9] [10]. CRAMM (CCTA Risk Analysis and Management Method) is an automated method based on a qualitative assessment. The method is comprising and flexible, and is specialized to motivate priority measures. To reach good results the method demands qualified and experienced personnel. CRAMM is a qualitative risk analysis method.

CRAMM is a method that is useful in all kinds of organizations. Here the essential elements of data collection, analysis and output results are present. The aim for this method is to justify security or contingency related investments for information systems and networks. This is done by demonstrating a need for action at the managerial level, based on quantifiable results and countermeasures from organization-specific risk analysis the method focus mostly on three things, namely:

- Identifying and valuing assets.
- Identifying threats and vulnerabilities, calculating risks.
- Identifying and prioritizing countermeasures.

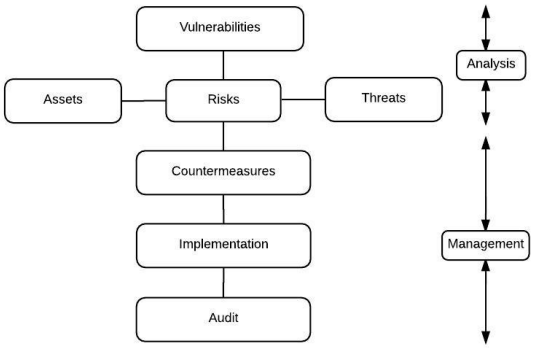

Figure 2: The approach of CRAMM

Initiation
CRAMM includes meetings, interviews and structured questionnaires for data collection. The method starts with a meeting were the reviewers and management of the company are involved. In this phase the goal is to identify and set realistic and important goals, set the scope and boundary of the analysis, design a project structure, come up with a schedule, and finally identify interviewees. The results are then documented in a so-called "Project Initiation Document". It can be hard but at the same time important to deliver a good asset analysis. If this is made too rough some important assets can be missed, and therefore causing misleading results.

Identification and valuation of assets
The next step is to evaluate these assets, which can be a speculative activity since it depends on by whom and when this is being done. To raise the level of organizational acceptance of the review when valuation of information assets is regarded, the reviewer conducts interviews with the "data owners" (for example business unit managers). To value the assets is a central role in the analysis since the continued work towards deciding the risk and the required security level is highly dependent on this.

The values are derived from the effects of crime against the accepted principles of information security: confidentiality, integrity and availability. The ones that are being interviewed states the worst-case scenario and outline the possible consequences of the data being unavailable, destroyed, disclosed or modified. This approach is considered as a deficiency in the method, since the worst-case scenario rarely occur in real life. The impact of the effect is defined and later compared with an appropriate guideline. This guideline provides the assets with a value which is placed within the scale of 1 to 10, where these number present the consequences.

Threat and vulnerability assessment
In addition to these asset values, there are two other imported components in CRAMM, namely an analysis over the probability that a threat will occur and the vulnerability after a threat has occurred. Threats and vulnerabilities are investigated against selected groups of assets. The assets are grouped together to facilitate the analysis and reduce the time.

In this stage predefined tables for combinations of threat/impact and threat/asset group is created. Depending on the customers need, the reviewers choose suitable threats and assets to investigate. It is not possible to perform an assessment of every threat to every asset group.

To assess the threats and vulnerabilities, threats and vulnerabilities are identified through questions from structured questionnaires that are presented to support personnel. These answers are taken into account were levels of threats against assets are calculated in a five point scale of "Very Low, Low, Medium, High, Very High" for the threats. The likelihood element is implied in the questions for assessing threats and vulnerabilities.

Risk calculation
When the analysis has reached the calculation stage, the risk of every asset group is calculated for every threat it is vulnerable against. The result presents of a number in a seven-graded scale. A comparison between the asset values and threat and vulnerability levels is made to calculate the risk. On this scale, "1" indicates a low level of security requirement, while "7" indicates a very high security requirement.

Before the last step can be entered, management needs to agree with and approve of the results. A review meeting with the management is appropriate.

CRAMM risk management
Based on the results the method produces a set of countermeasures applicable to the system, which are considered necessary to manage the identified risks. A recommended security profile will then be presented and thereafter compared against existing countermeasures to identify areas of weakness or over-provision. Countermeasures are placed in groups and subgroups based on security aspects. Each countermeasure is dedicated a security level from a seven graded scale, were 1 stands for very low, and 7 means very high. This value is decided through a comparison of risk measures. If a countermeasure gets a high value, this leads to a high priority to evaluate that particular countermeasure.

The last activity in the analysis is to present it to the management. This means presenting a summery of the findings and conclusion of the risk analysis that has been made. It also consist of an explanation of recommended countermeasures that gives a broad indication of the priority and costs involved when implementing them. Still CRAMM does not provide documentation telling how effective each countermeasure will be. The management is responsible of the final decision to implement, enhance or remove countermeasures.

2.2.3 ISRAM

Our description of ISRAM is based on the following references: [2] [11].
ISRAM is a quantitative paper-based risk analysis method, where the aim is to assess the risks caused by the information security problems in today's complex information systems. The method is built upon the fundamental risk formula:

Risk = (Probability of occurrence of security breach)×(consequence of occurrence of security breach)

The method consist of seven steps where opinions from people such as managers, directors, technical personnel and common system users are taken into account by conducting a survey. This survey includes questions associated with the specified information security problem and a group of answer choices are connected to each question. The aim of the survey is to asses the risks and understand the affect of them in the systems. The different steps of the ISRAM method is presented in Figure 3.

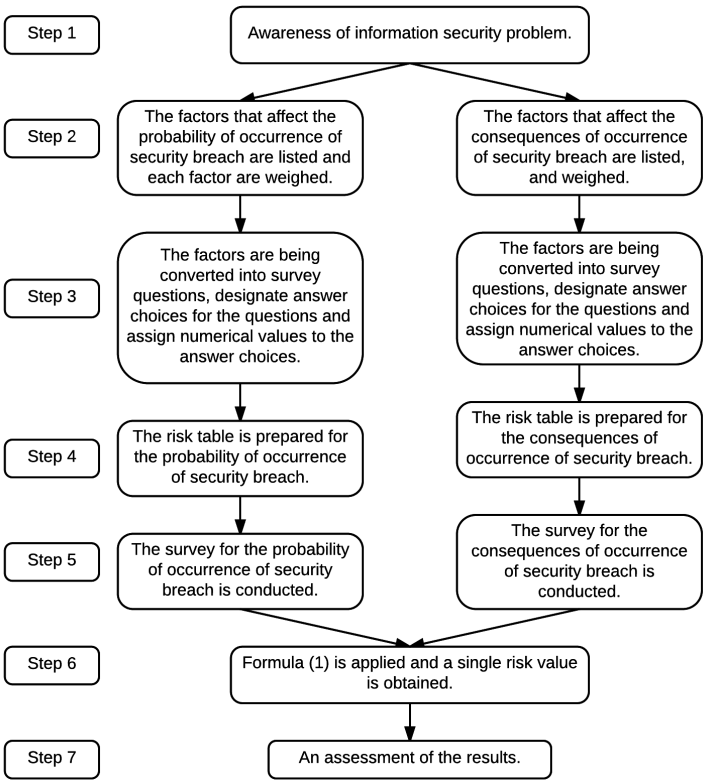

Figure 3: The steps of ISRAM

Step 1
In the first step the awareness of the problem is identified. The questions and the answer choices are formed and the risk tables are prepared. In this stage the existence of security problems are detected. When this is done the process is divided into two parallel sub-processes, which will consist and be performed simultaneously until the end of the analysis. One of the sub-processes handle the probability of occurrences of different security risks, while the other one handle the consequences of the occurrences.

Step 2
The analysis is now ready to enter step two. Here an identification of all factors that might affect the probability of threats against the system is made. The factors are listed and thereafter given a weighted value depending on how the attack will affect the probability of an occurrence of a security breach. At the same time in the simultaneous process, all consequences are identified and weighted. It is not necessary that the number of consequences is the same as the probability factors. To keep the results of the analysis objective and realistic, step two is a vital part of ISRAM.

Step 3
In the third step, the factors for both the consequences and probability are subsequently converted into the survey questions. The answer choices are also determined for each of the questions. Each answer is weighted and given a value. It is very important that the answers choices are well thought out and designed since the answers from the participants will be the prime assets to the analysis. Therefore it is also vital that the answers from the participants are well thought.

Step 4
Now the analysis will initiate step four where two risk tables are prepared. These are made by the results of the survey. These tables prevent confusion in the quantitative analysis, and lays a foundation so that the outcoming results for the analysis will be concrete and useful. The risk tables are formed by the values of the answers. The maximum values the questions of the probability can give as well as the minimal value are calculated. Then an interval is created so that the questions can be converted to a scale. This is also done for the consequences.

Step 5
In step five, the survey is carried out. The questions are distributed between the participants, i.e. managers, directors, technical personnel and common system users.

Step 6
In step six the ISRAM equation 1 is applied to receive quantitative risk results from the completed survey.

$$Risk = \left(\frac{\sum_{m=1}^{N}\left[T_1\left(\sum_{i=1}^{I} w_i p_i\right)\right]}{m}\right)\left(\frac{\sum_{n=1}^{N}\left[T_2\left(\sum_{j=1}^{J} w_j p_j\right)\right]}{n}\right) \quad (1)$$

- i: the number of questions for the survey of probability of occurrence, determined at Step 2.

- j: the number of questions for the survey of consequences of occurrence, determined at Step 2.
- m: the number of participants who participated in the survey of probability of occurrence, becomes definite at Step 5.
- n: the number of participants who participated in the survey of consequences of occurrence, becomes definite at Step 5.
- wi, wj: weight of the question "i" ("j"), determined at Step 2.
- pi, pj: numerical value of the selected answer choice for question "i" ("j"), determined at Step 3.
- T1: risk table for the survey of probability of occurrence, constructed at Step 4.
- T2: risk table for the survey of consequences of occurrence, constructed at Step 4.
- Risk: single numeric value for representing the risk. Obtained at Step 6.

Step 7
The final step of ISRAM is often called the assessment phase. In the assessment phase not only the numerical results of the investigation we can see in step six, but also the ultimate risk is assessed based on analysis of survey questions.

2.2.4 OCTAVE Allegro

OCTAVE stands for "Operationally Critical Threat, Asset, and Vulnerability Evaluation". OCTAVE methods are flexible and self-directed. With the use of OCTAVE, small teams across business units and IT can work together to address the security needs of their organization. The method can be tailored to an organization's unique risk environment, security and skill level. "OCTAVE moves an organization toward an operational risk-based view of security and addresses technology in a business context." [12] OCTAVE Allegro is the most recently developed and actively supported method. This method is based on two older versions called OCTAVE Original and OCTAVE-S. The original OCTAVE method was created in 1999 by the Software Engineering Institute located at Carnegie Mellon University in Pittsburgh, Pennsylvania. In this review we will focus on OCTAVE Allegro which was created in 2007 [13].

The main focus of OCTAVE Allegro is information assets. The important assets in an organization are identified and assessed based on the context of how they are used, where they are stored, transported, processed, and how they are exposed to threats, vulnerabilities and disruptions as a result. This process helps reducing the possibility that major data gathering and the analysis are performed for assets that are not well defined. One of the advantages of using OCTAVE Allegro is that it can be performed in a workshop-style, collaborative setting and is supported with all the needed guidance, worksheets, and questionnaires, which are all available online for free. The method is also appropriate for use by individuals who want to perform risk analysis without extensive organizational involvement, expertise, or input.

OCTAVE Allegro consists of eight steps organized into four phases, as illustrated in Figure 4. The steps are similar to the steps used in the CORAS methodology (Section 3.3.8). The four phases are:

1. The organization develops risk measurement criteria based on organizational information.
2. Information assets that are determined to be critical are profiled. This profiling process establishes clear boundaries for the asset, identifies its security requirements, and identifies all of the locations where the asset is stored, transported or processed.
3. Threats to the information assets are identified in the context of the locations where the assets are stored, transported or processed.
4. Risks to information assets are identified and analyzed and the development of mitigation approaches is commenced.

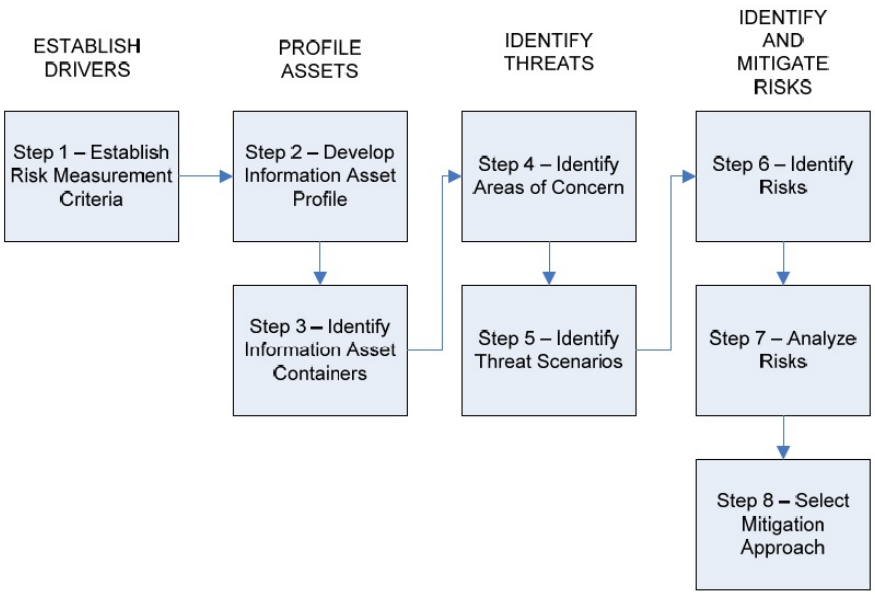

Figure 4: The eight steps of OCTAVE Allegro

The outputs from each step in the process are captured on a series of worksheets which are then used as inputs to the next step in the process. To get a better understanding of the eight steps of OCTAVE illustrated in Figure 4, here's a brief summary [13]:

Step 1
A set of risk measurement criteria is created as part of this initial step. Risk measurement criteria are a set of qualitative measures against which the effects of a realized risk can be evaluated and form the foundation of a risk analysis. Step 1 also includes assigning a priority to the organization's impact areas, such as the relationship with customers and compliance with regulations. Depending on the organization, an impact to the relationship with customers may be more significant than an impact on its compliance with regulation.

Step 2
OCTAVE focuses on the information assets of the organization and in step 2 begins the process of creating a profile for those assets. A profile is a representation of an information asset describing its unique features, qualities, characteristics and value. The profile for each asset is captured on a single worksheet that forms the basis for the identification of threats and risks in subsequent steps.

Step 3
Containers describe the places where information assets are stored, transported and processed. Information assets reside not only in containers within an organization's boundaries but they also often reside in containers that are not in the direct control of the organization. Any risks to the containers in which the information asset lives are inherited by the information asset.

Step 4
Step 4 begin the risk identification process by brainstorming about possible conditions or situations that can threaten an organization's information assets. These real-world scenarios are referred to as areas of concern and may represent threats and their corresponding undesirable outcomes.

Step 5
The areas of concern captured in the previous step are now expanded into threat scenarios that further detail the properties of a threat and a broad range of additional threats are considered by examining these threat scenarios.

Step 6
In step 5 threats are identified, and in step 6 the consequences to an organization if a threat is realized are captured, completing the risk picture.

Step 7
In step 7 of this assessment, a simple quantitative measure of the extent to which the organization is impacted by a threat is computed. This relative risk score is calculated by considering the extent to which the consequence of a risk impacts the organization against the relative importance of the various impact areas, and possibly the probability.

Step 8
In step 8, the final step of the OCTAVE Allegro process, organizations determine which of the risks they have identified require mitigation and develop a mitigation strategy for those risks. This is accomplished by first prioritizing risks based on their relative risk score.

2.2.5 COBRA

COBRA stands for Consultative, Objective and Bi-functional Risk Analysis and was created in 1991 by C & A Systems Security Ltd. COBRA was designed to give organizations the means to perform a self-assessment of their IT-security without the need for external assistance from consultants. The fact that IT security can be looked at as a business issue, rather than primarily as a technical one, has led to the development of the COBRA method. It was, and is, becoming largely expected that security reviews should be business related, with cost justified solutions and recommendations [14].

COBRA follows the guidelines set forth by ISO 17799 [15], and its methodology is not so much a documented process as a downloadable program that consists of two parts: COBRA Risk Consultant and ISO Compliance. COBRA Risk Consultant is the default program to use when it comes to the COBRA method. ISO Compliance is only used when ISO17799 specifically needs to be taken into account. Both sub-applications are customisable and use knowledge bases containing expert knowledge to aid the user in analysing their security risks [16].

Risk Consultant is a questionnaire based computer program and comes with standard questions for gathering the types of assets, vulnerabilities, threats, and controls that are in place in an organization. It evaluates the relative importance of all threats and vulnerabilities and generates appropriate recommendations and solutions. In addition, its reports provide a written analysis and relative risk score for each risk category. The risks identified are automatically linked with the potential implications (financial, customer loss, etc.) for the business or department. An important part of the Risk Consultant program is the option to customise the knowledge base from which the program gathers its information. This enables question modules to be directed at personnel with the appropriate expertise and knowledge. As well as increasing accuracy, this approach enables more detail and precision and thus ensures better results and solutions. "COBRA Risk Consultant is designed to be truly self-analytical. It can be used without the need for detailed security knowledge or expertise in using risk management software. There is no need to hire expensive consultants to back-up the system" [17]. It is possible to change the value of the variables in the program, making it easy to see "If this value goes up by 25%, how will it affect the overall outcome of the analysis?". The reports produced by Risk Consultant are professional business reports, which are suitable for interpretation by both technical and non-technical personnel.

ISO Compliance comes with standard questions which assess the major categories specified in the ISO 17799 standard. As with Risk Consultant, it can provide an assessment of an organization's compliance and suggest steps for action [16].

COBRA's default process consists of three stages:

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

The following specifications of the different stages are summarized by C & A Security Risk Analysis Group [18]. During the first stage, via module selection or generation, the base questionnaire is built to fit the environment and requirements of the user. Each selected module embraces a particular area of risk or a specific threat class, e.g. Logical Access, Physical Access, Networks, Development, Operations, etc. Building the questionnaire can be done manually or automatically. With an automatic questionnaire build, the system creates a questionnaire that suits the user's system/installation specifically. This is achieved through completion of the initial "Business" or "Impact" Questionnaire. A manual questionnaire build may be desirable for a variety of reasons:

- Consideration of a specific aspect of security/risk.
- Performing risk analysis in various proposed scenarios.
- Analysis of all risk areas, even if some are not of real significance to the organization.

The second stage is the survey process - Risk Consultant questions are answered by appropriate personnel and the information is securely stored. Questions are of various formats; mandatory single response, optional single response, mandatory multiple response, optional multiple response, text response, and numeric response. Most are of a simple, multiple choice variety. Further question modules may be dynamically generated as questions are answered and Risk Consultant obtains more information.

For the third stage risk assessments and "scores" are produced for individual risk categories, individual recommendations are made and solutions offered, and potential business implications are explained. A number of report sections are provided:

- Recommended solutions and specific additional security control suggestions.
- A descriptive assessment and relative risk score for each "risk category" in each area considered.
- A full impact analysis for the business or department.
- Direct linkage between areas of risk and the potential financial and business implications.

2.2.6 Mehari

Our description of Mehari is based on the following references: [19] [20] [21]. Mehari is a method used to provide a set of tools for security management. The approach of Mehari consists of these four steps:

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

The method includes a set of actions, where each and every one has their own specific goal. Some examples of 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.

All these actions considered, the main goal of Mehari is to make a risk assessment and reduce these risks. Mehari is knowledge based and its mechanisms and tools were created for that purpose. The method also provides a guideline for making a security assessment. This is done in nine steps, which will here be described briefly.

Step 1
The first step of Mehari includes an identification of risks. This could be done in two ways.

1. An identification of malfunctions or potential events is done in the operational processes of the organization. These events will be put in a malfunction value scale, which provides a value of the risks. The first step will give knowledge of what kind of malfunctions that can occur, a definition of the parameters that affects the risks, and thereby the malfunction and an evaluation of the critical parameters that increase the malfunction.
2. An organized, systematic and automated evaluation created by using a scenario base. The method provide a comprehensive knowledge base for these automated valuations. An audit form, provided by Mehari is used as a knowledge base for performing these security risk assessments.

Step 2
In this step a threat evaluation is made. Here a scale of four grades is used to decide the impact of the threats.

- Level 1: Very low exposure. Independently of any security actions. The probability of occurrences is negligible.
- Level 2: Low exposure, even if non security actions are taken. The combination of environment and the context make the probability of occurrences low.
- Level 3: Medium exposure. If no actions are made, the probability of occurrences in short term is quite high.
- Level 4: High exposure. If nothing is done to avoid this, it will occur for sure.

Step 3
In step three an evaluation of deterrent and preventive factors that can prevent the risks to occur is made.

Step 4
This step includes an evaluation of the protective and restoration factors that can be done after a risk has occurred.

Step 5
In this step there will be an evaluation whether a risk has potential to occur, or not. Questions like "How likely is the occurrence of the risk being analysed." and "Is that scenario complete and creates real damage?" are brought up. Here a scale of five levels is being used.

- Level 0: Not considered. These are scenarios that are so impossible that they will not be included in the set of scenarios that are being analysed.
- Level 1: Very unlikely. The occurrence of the risk is totally improbable.
- Level 2: Unlikely. These are scenarios that often can be considered as not happening.
- Level 3: Likely. Scenarios that could happen.
- Level 4: Very likely. Scenarios that will occur with quite certainty.

Step 6
In this step an evaluation of the intrinsic impact is made. That means the evaluation of the consequences of the risk events that are actually happening. In Mehari this is made by filling in an intrinsic impact table. This table can further be used for the evaluation process.

Step 7
Now it is time to evaluate the impacts. This evaluation is made in two steps:

- Evaluation of an impact reduction indicator.
- Impact evaluation.

Step 8
From the outcoming result in step seven a global risk is defined in step eight.

Step 9
The final step in Mehari is to determine whether the risk is acceptable or not. If the risk is evaluated as a non-acceptable risk, a control mechanism further needs to be developed to prevent the risk from occurring.

2.2.7 Magerit

Our description of Magerit is based on the following references: [20] [22]. From the beginning Magerit was prepared and promoted by the CSAE (Consejo Superior de Administracion Electronica) in response to the perception that the government (and in wider terms, society) increasingly depends on information technology to achieve its service objectives. But nowadays the method is used in organizations all over the world. The goals of Magerit are:

- To make those responsible for information systems aware of the existence of risks and of the need to treat them in time.
- To offer a systematic method for analysing these risks.
- To help in describing and planning the appropriate measures for keeping the risks under control.
- To prepare the organization for the process of evaluating, auditing, certifying or accrediting, as relevant in each case.

Magerit includes five steps which are illustrated in Figure 5.

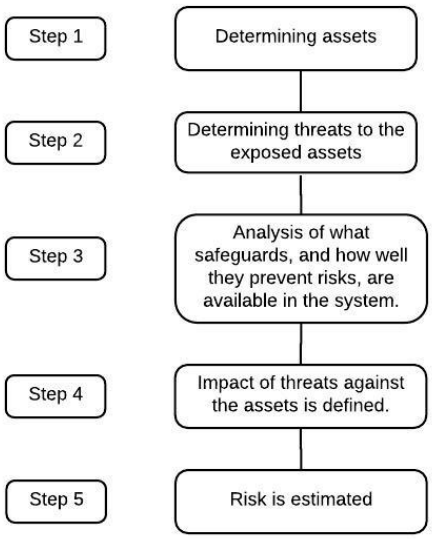

Figure 5: The five steps of Magerit

Step 1
The first approach is, as in most risk analysis methods, to determine an organization's relevant assets. But they are not only determined, an inter-relationship between them, and their value is also determined. Assets in Magerit are defined as the resources in the information system, necessary to make the organization operate correctly. One of the essential assets is information handled by the system, with other words the data circulating within the system. Other relevant assets could be the following:

- The services that can be provided to these data and the services needed to be able to manage these data.
- The computer applications (software) that allow these data to be handled.
- The computer equipment (hardware) that hosts the data, applications and services.
- The information media, which are data storage devices.
- The auxiliary equipment that complements the computer equipment.
- The communication networks that allows for the exchange of data.
- The installations that houses the computer and communications equipment.
- The personnel who use or operate all the elements above.

Step 2
In the second step the threats to the exposed assets are determined. By threats it means things that might occur and then could cause damage to these assets. The threats can be of different characters, they may be from natural disasters or industrial accidents. The threats may also come from a person and whether it is by purpose or not, it can cause damage to the organization's assets.

Step 3
The third step includes analysing what safeguards that are available in the system and how well they prevent risks. By safeguards it means a procedure or technical mechanism that reduce risks. Some risks can more easily be removed by using suitable organizational mechanisms. Other may require technical devices, physical security or personnel policies.

Step 4
In the fourth step the impact of the threat occurrence against the asset is defined. This is a measurement of the asset-damage the threat will create. This value together with value of the asset, the total impact on the system can be calculated.

Step 5
In the fifth and last step the risk is estimated, this is defined by the weighted impact on the rate of occurrence of the threat, or the expectation of appearance of the threat. By risk it means the likely damage to the system. After the

impact on the system has been estimated (step 4) the risk can be calculated. This is done by including the frequency of occurrence. With a high frequency and big impact the risk will increase.

2.2.8 CORAS

CORAS is a qualitative risk analysis method which provides a customized graphical language for threat and risk modelling. The CORAS method consists of seven steps and comes with detailed guidelines explaining how the graphical language should be used to clarify and model relevant information throughout the whole risk analysis process. The Unified Modelling Language (UML) is typically used to model the target of the analysis. For presenting the overall conclusions special CORAS diagrams are used, which are inspired by UML. The CORAS method also provides a computerized tool [23]designed to help create these diagrams. The symbols in Figure 6 are used in the CORAS diagrams to cover both technical and more high-level information, making it easier for people with different competences to understand the different steps of the risk analysis. A common basis for communication reduces misunderstandings and thereby gives a more correct risk picture. The documentation created by the CORAS method is produced so that it should be more or less self-explanatory, and not rely on extensive training to be understood.

Figure 6: CORAS symbols

The developers of CORAS claim that this graphical approach to risk analysis contributes to solving three common issues related to risk analysis methodologies [24]:

- How to facilitate communication in a group consisting of people with different backgrounds and competences.
- How to estimate the likelihoods and consequences of identified risks.
- How to document the security analysis in a comprehensible manner.

The seven steps of CORAS are summerized here by F den Braber, I Hogganvik, M S Lund, K Stølen and F Vraalsen [25].

Step 1 – introductory meeting
The first step involves an introductory meeting. The main item on the agenda for this meeting is to get the representatives of the client to present their overall goals of the analysis and the target they wish to have analysed. Hence, during the initial step the analysts will gather information based on the client's presentations and discussions.

Step 2 – high-level analysis
The second step also involves a separate meeting with representatives of the client. However, this time the analysts will present their understanding of what they learned at the first meeting and from studying documentation that has been made available to them by the client. The second step also involves a rough, high-level security analysis. During this analysis the first threats, vulnerabilities, threat scenarios and unwanted incidents are identified. They will be used to help with directing and scoping the more detailed analysis still to come.

Step 3 – approval
The third step involves a more refined description of the target to be analysed, and also all assumptions and other preconditions being made. Step three is terminated once all this documentation has been approved by the client.

Step 4 – risk identification
This step is organised as a workshop, drawn from people with expertise on the target of the analysis. The goal is to identify as many potential unwanted incidents as possible, as well as threats, vulnerabilities and threat scenarios.

Step 5 – risk estimation
The fifth step is also organised as a workshop. This time with the focus on estimating consequences and likelihood values for each of the identified unwanted incidents.

Step 6 – summary
This step involves giving the client the first overall risk picture. This will typically trigger some adjustments and corrections.

Step 7 – risk treatment
The last step is devoted to treatment identification, as well as addressing cost/benefit issues of the treatments. This step is best organised as a workshop.

Brainstorming is a valuable tool while working with CORAS, especially for the workshops mentioned in steps four, five and seven where people with different backgrounds and competences are working together to find new angles to work with. Figure 7 is an example of what a CORAS diagram from step seven can look like. The scenarios explained by this figure illustrates what kinds of treatment that could be used to protect the assets from different kinds of deliberate human threats.

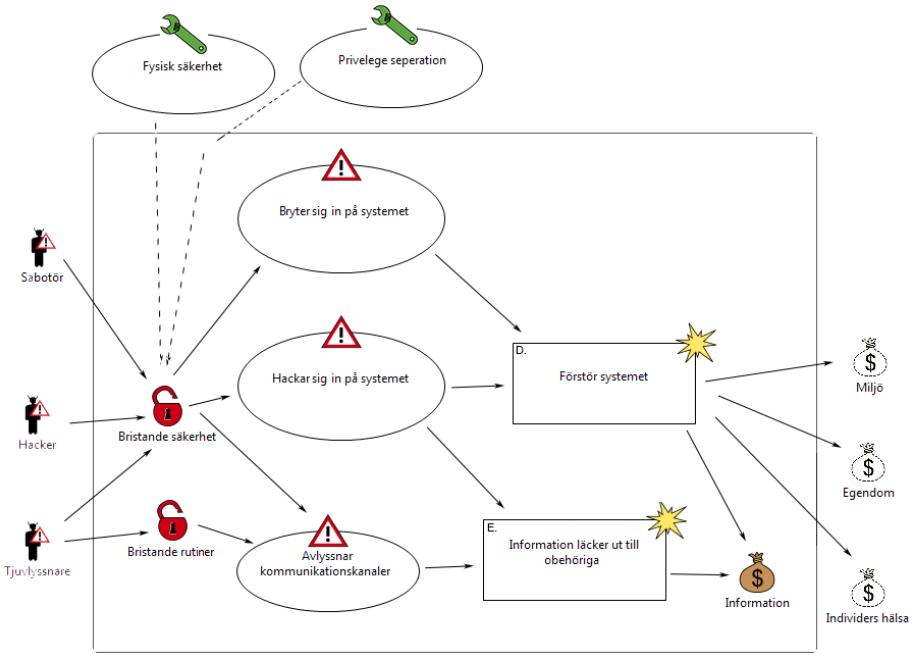

Figure 7: CORAS step seven example

3 Methodology

The first thing that we needed to do to be able to write this review was to find several different risk analysis methods. Our strategy to find methods was to browse comparative studies of risk analysis methods. The studies we found then led us directly to different risk analysis methods [4]. Going through the bibliography of these studies turned out to be rewarding, since it led us to more detailed information regarding the methods. We also used multiple resources to locate more methods and to find detailed information about them, such as Google Scholar [5] and UniSearch [6]. During our search for methods we used the search terms "risk analysis method", "comparison of risk analysis methods" and "different risk analysis methods". We decided to mainly focus on methods that had free and published documentation. Once we had found eight methods to include in our review we used multiple databases to get more information about them. The databases we used were: ScienceDirect, Scopus, Inspec and Manuscriptorium Digital Library.

3.1 Classification of risk analysis methods

All risk analysis methods in this review calculates and compares risks and tries to provide the best possible countermeasures or at least the most accurate suggestions on what to do next. The methods do this in their own unique way and the results vary, but they still share the same structure which can be explained by four different steps. The first step is to identify the assets in the system. Step two aims at finding possible threats against the identified assets. After that is done, step three is to quantify the risks with the help of the basic risk formula $Risk = consequence \times probability$. Modified versions of the formula may occur, but they are all based on consequences and probability. The fourth and final step is the countermeasure step. At this step countermeasures are developed to mitigate the identified risks.

To help future organizations and people performing risk analyses, we have classified our 8 different risk analysis methods by a chosen set of criteria. Our classification points out some of the pros and cons for each method, making it easier to choose the one best suited for a specific scenario.

The classification for the eight risk analyses we summarized in Section 3.3 is based on four main areas. This facilitates the choice of risk analysis for an organization, since the aim and expectation of an organization's risk analysis can be compared with our classification which will thereby point out the most appropriate method.

The four main areas are:

- Resources.
- Focus on one versus several problems.
- Qualitative versus quantitative.
- Decision support.

Resources
In this category the scope of resources when it comes to different persons, time, specific equipment (where both hardware and software are included) and the amount of deadlines are taken into consideration. The scale for resources is divided into either "high" or "low", with a high rating meaning that the analysis will take a considerable amount of time, require a lot of personnel and/or specific equipment and include several deadlines and mandatory meetings regarding different stages in the analysis. A low rating stand for the opposite.

Focus on one versus several problems
This area takes into account whether the analysis method discusses and focuses on one or multiple problems at the same time. The scale consists of "one" or "several".

Qualitative versus quantitative
A method can be either qualitative, quantitative or a mix of them both. The scale is therefore divided into three sections: "qualitative", "quantitative" and "both". A quantitative method involves interpreting numbers from data and estimates and is most likely a mathematically based analysis. A qualitative method involves interpreting interviews, words and images [1].

Decision support
The scale for decision support is divided into either "high" or "low". The meaning of this is how concrete information the method gives regarding the choice of mechanisms that are needed to mitigate the risks. A method with high decision support states clearly what is needed to be done to mitigate the risks that were found earlier in the analysis. A method with low decision support gives negligible, or no, suggestions on what to do to mitigate the risks.

3.2 Conducting the interviews

We conducted interviews with experts in IT-security to get professional opinions regarding risk analysis methods and what important factors there are to keep in mind while performing risk analyses. We contacted several different companies and tried to get in touch with the IT-security experts in respective companies. Thereafter we set a date and place and met up for the interviews. All interviews took place in company located meeting rooms. We created the interview questions (see Appendix A) based on our classification, and on information regarding the risk analysis methods presented in Section 3. We emailed the questions to each company one week before each scheduled interview to make it easier for them to prepare. We interviewed representatives from Ericsson, SAAB and Tage Rejmes Bil AB. Each expert has provided us with information regarding how IT-security is handled in their respective companies, and they will be anonymous in this report.

3.3 Previous documented usage of risk analysis

In Section 2.1 we mentioned that the secondary aim of this review is to find scientific applications and real world usages of risk analysis methods, and if possible connect these with our classification. To do this, we searched for published documented usage of risk analyses from companies and organizations to see what results their analyses led to. At first we used wider search terms "practical usage of risk analysis" and "risk analysis, company used" on Google Scholar [5] and the UniSearch [6] search tool. This did not lead to any useful results so we decided to fall back to simpler search terms, like "we used *method*" where *method* was substituted with the name of each of our eight methods. This search resulted in two published documents, one describing a CISO team at European Commissions usage of attack trees and the other describing how the top management of a large Czech company used CRAMM.

4 Results

In this section we will present the results from our classification of risk analysis methods, interviews and previous documented usage of risk analysis.

4.1 Classification of risk analysis methods

Table 1: Resources

Low	**High**
Attack trees	CRAMM
OCTAVE	ISRAM
COBRA[1]	Mehari
Magerit	CORAS

Table 2: Focus on one vs several problems

One	**Several**
Attack trees	CRAMM
ISRAM	OCTAVE
	COBRA
	Mehari
	Magerit
	CORAS

The methods that focus on several problems can all be configured to treat only one problem at a time, but not the other way around.

Table 3: Qualitative vs Quantitative

Qualitative	**Quantitative**	**Both**
Attack trees	ISRAM	OCTAVE
CRAMM	COBRA	Mehari
Magerit		
CORAS		

[1]COBRA does require the purchase of several programs to function properly. But after that is done, the amount of resources needed to use the method is considered to be "low".

Table 4: Decision support

Low	**High**
Attack trees	OCTAVE
CRAMM	COBRA
ISRAM	CORAS[2]
Mehari	
Magerit	

4.2 Interviews with IT-security experts

When asked to define the term "risk analysis" the experts told us that for them it is a structured way to identify, evaluate and handle risks. It is important to discover the critical factors in each system and find solutions to mitigate the risks, or if that is not possible, at least create an action plan. It is also important to set up boundaries and make priorities so that you do not waste resources.

Since our report focuses on finding and classifying risk analysis methods we asked all the experts what methods they use to keep their systems safe. At Ericsson, they use their own methods that are tailored to their specific needs. Without revealing too much, their standard risk analysis methods starts with brainstorming to find all possible risks. Then they guess the probability and consequence for each and every risk, and finally decide what actions to take. Rejmes on the other hand does not develop their own methods like Ericsson does. Instead they buy their systems from external service companies and it is these companies responsibility to keep the systems safe. One kind of risk prevention that is used at SAAB, Rejmes and Ericsson is penetration tests, where security personnel try to break into systems and thereby finding its weaknesses. When SAAB is about to deploy a new system they use a four step process to see if the system is safe. The steps are:

1. Create a system description and clarify which conditions are relevant.
2. Identify requirements and perform a risk analysis.
3. Check if the requirements are met.
4. Make a risk based decision to decide if the system should be deployed or not.

All three companies perform qualitative risk analyses more often than quantitative ones, but when it comes to mitigating one or several risks at once there were some differences between the three. The expert from Ericsson told us that they think in a "one catastrophe at a time"-kind of way, because they lack sufficient tools to add risk scenarios together. From Rejmes we learned that they only work with overarching risk analyses, because they have a need for constantly

[2]CORAS does provide several alternative ways to mitigate risks, but it does not indicate which alternative is the most efficient.

looking at the bigger picture. At SAAB they do most of their risk analyses in workshops, making it easy for them to adapt and focus on one or multiple risks at a time. The process of keeping the systems safe is a never-ending process at all three companies, due to new risks constantly emerging.

When it comes to protecting assets in the systems, both Ericsson, SAAB and Rejmes agree that information is the main asset. Without information, there is no company. Ericsson and SAAB which both handle classified information in another way than Rejmes, have classified all their information, making it easier to control who has access to what. There will be consequences if information gets into the wrong hands. To clarify these consequences, SAAB uses the following scale:

- Small damage to the company, no damage to 3rd party.
- Some damage to the company, damage to 3rd party.
- Large damage to the company, losing clients and market trust.

The one question where all the experts fully agreed was "what is the hardest thing to protect a system against?" to which they all answered: the human factor. Most of the time accidents leading to risks occur without intent from employees. They can find themselves in a stressful situation which makes them take short cuts to meet a deadline, even though it will mean bypassing some sort of company security. The best way to prevent these kinds of risks from happening is to educate employees, making them aware of current security protocols and what happens when they are not followed. But if an employee is trusted by the company, yet decides to steal information or destroy a system on purpose, it is almost impossible to prevent that from happening.

When it comes to the amount of resources that each company spend on threat protection and making risk analyses, both Ericsson and Rejmes agrees that compared to other parts of the business, they do not spend a lot of resources (personnel, time and money) on threat protection and risk analyses. SAAB on the other hand spend a bit more on these areas compared to the rest of their business, which is understandable considering the fact that they work with matters of national security. At SAAB there are both internal personnel and external consultants working with IT-security. Rejmes has 4 out of their 635 employees working full time with IT-security and at Ericsson in Linköping there are a handful.

Finally we asked each of the experts what the most important things while performing a risk analysis are. They all stressed the fact that you need to focus on what output you want from your analysis so you can use available resources in the best possible way. It is also important to know who is in charge of what in the company and assigning dedicated owners to every piece of information is a good start.

4.3 Previous documented usage of risk analysis

In this section we will present two examples of real world usage of risk analysis methods. This will provide a quick look at some of the methods that are being used by companies today.

4.3.1 Attack trees

The reason that a team at the European Commission used the attack tree-methodology was that they wanted to perform a broad and detailed threat analysis and not disregard anything. To discover the threats that are later placed in the attack tree structure, they used a threat modelling technique called STRIDE [26], which resulted in about 70 relevant threats regarding the information technology system. The team who performed the analysis had a set of positive comments regarding attack trees. And after they used the method on their system, and were given the results of it, they summarized the attack tree methodology as [27]:

- Flexible - can be used on any kind of system.
- Visual - which results in good communication.
- Formal - it has appropriate formal properties.
- Attack scenarios - it provides incident scenarios.
- Brainstorming tool - accessible and easy to use as a brainstorming tool.

4.3.2 CRAMM

A risk analysis, were the aim was to establish and operate a Information Security Management System (ISMS), was performed by a large Czech company. ISMS is a set of policies regarding the management of information security and IT-related risks. The basic principle of the policies is that an organization should design and maintain guidelines to handle the risks against their information assets. The reason that the company decided to use the CRAMM method was that it had several successful certifications and satisfied users, and that it is a method well known in Europe. The methods countermeasures library and security documentation is primarily well suited for operating ISMS.

To gain the most out of the analysis, the management together with the security department specialists took usage of external expertise from a consultancy firm for assistance. Therefore the work was performed through close cooperation between these parties. Thanks to this approach, and the methodology of CRAMM, the limited resources the company had were used effectively.

The result of the analysis showed weaknesses in the security of the system. Therefore the continued work of the project was to implement countermeasures to these problems. The aim of the project was to improve the level of security in the system. Based on the recommendations that CRAMM gave, physical security was upgraded [28].

5 Discussion

In this section we will discuss and criticize our methodology. We will do this by examining our results and comparing them with the theory presented in Section 3. We will also discuss some of the ethical perspectives of our work.

5.1 Methodology

The first thing we noticed while searching for risk analysis methods to include in our review was that the amount of information available for the methods varied heavily. Methods such as CORAS and ISRAM had a lot of online documentation which gave an in-depth explanation for each method. Methods like Magerit on the other hand, were hard to find in-depth documentation for and the documentation that we did find merely gave a short overview of the method. There are a lot of reviews available online regarding risk analysis methods, but none that we found really gave a good description of the methods. The reviews we found all focused on listing methods, a lot of them, instead of describing them. With our review we focused more on the describing part, making our review a guideline for choosing the most appropriate method. The way we chose our methods was to look for methods that had documented information from a reliable source, and not really focus on the amount of information available. This is something we would do differently if we were to write another risk analysis review. A better approach would be to chose methods based on both reliable sources and the amount of available documentation, making it easier to find both overviews and in-dept explanations. The easiest way to make the review more comprehensive is to add more methods. Considering the amount of time available for making this review we chose to include eight methods.

Our classification focuses on the four areas that we found most important: resources, focus on one versus several problems, qualitative versus quantitative and decision support. These areas were subjectively chosen by us and may not provide the best and complete information. One way to provide a classification more suited for a specific organization would be to develop the classification together with representatives from that organization. This way the review will have the correct focus from the start. Another way to improve the review is to expand the classification, by adding more parameters.

Finding companies to interview turned out to be relatively easy but we did not take into consideration the amount of time it would take to actually schedule an interview. While planning our interviews we thought that if a company agreed to schedule an interview, the interview would happen. This was not the case. Due to reasons unknown to us two interviews got cancelled. We have learned that scheduling and conducting interviews takes a lot more time than one might think at first. Finding previous documented usage of risk analysis was a lot harder than we anticipated, because people do not tend to publish documentation on how they are using risk analysis methods. It is easier to find documentation telling what methods that were used, but not how they were used.

Considering the reliability of our review, it is likely that another review done with our parameters and by our methodology would lead to similar results. Our description of the eight different methods are based on reliable sources (in most cases the developer of the method), making the validity of this review high.

5.2 Results

The tables in Section 5.1 illustrates that the eight methods are quite evenly distributed between the different columns, except for in table 2. This is the case due to us almost exclusively finding methods developed to fix several problems instead of only focusing on a particular problem. One thing that we did not anticipate was that most of the methods does not provide high decision support. When we started writing this review we thought that all risk analysis methods would clearly state what actions are necessary to mitigate the risks.

Instead of using specific risk analysis methods, the companies had developed their own methods to suit their specific needs. Although some of these self developed methods were based on parts from different well known risk analysis methods. At each interview, we quickly understood that the area of risk analysis is a company secret and we did not always get as comprehensive answers as we hoped for. If we look at the type and structure of the companies we interviewed (Ericsson, SAAB and Tage Rejmes Bil AB) we could see that Ericsson and SAAB are quite similar in how they work with risk analysis. This is something that we anticipated, mostly because they both are large engineering focused companies. Rejmes on the other hand works in a completely different area, the car sales industry, making it completely understandable that they have a different way to look at risks than Ericsson and SAAB.

When we looked at previous documented usage of risk analysis methods, we did manage to find two cases where methods included in our review had been used. In the first case, with the use of attack trees, we noticed that they had followed the standard attack tree model and even used the same references as we had in our review [7]. In the other case, with the use of CRAMM, they had also followed the standard model of CRAMM. Due to the fact that both of these models had been used in real world situations, and produced satisfying results, we see that there really is a need for good risk analysis methods.

5.3 A broader perspective

The area of risk analysis is truly important to all companies and the methods they use are often classified and involves sensitive information. Due to the secrecy surrounding this kind of company sensitive information, we chose to let our three interviewees be anonymous throughout the review. We also contacted the interviewees and sent them our review before publishing it, so that they could approve of everything we decided to include. This was important for us to be able to write this review in an ethical way.

6 Conclusion

We have previously stated that the primary aim of this review was to survey scientific literature in order to find proposed methods and to suggest a classification of these methods in order to alleviate the choice of method. We have reached our primary aim and the proposed methods are described in Section 3.3 and our classification is located in Section 5.1. We also stated that our secondary aim was to find scientific applications and real world usages of risk analysis methods, and if possible connect these with the classification previously done. To reach our secondary aim, we have conducted several interviews in Section 5.2 and researched previous documented usage of risk analysis methods in Section 5.3. We have seen that larger companies tend to develop their own methods for risk analysis, which indicates that smaller companies are most likely the target group for this review. Companies that do not have enough time or resources to develop their own methods, and instead want to use already existing ones can use this review for guidance.

For the making of future risk analysis reviews we recommend including as many methods as possible, making the review more comprehensive. We also recommend including IT-security experts in the process of developing the classification.

References

[1] T. Norman. *Risk Analysis and Security Countermeasure Selection*, CRC Press, 2009.

[2] T. R. Peltier. *Information Security Risk Analysis*, CRC Press, 2010.

[3] A. Bhardwaj, *Analysis Paralysis: When to stop?*, arXiv:0903.5024 [cs.SE], 2009.

[4] F. Macedo, *Comparative Study of Information Security Risk* https://fenix.tecnico.ulisboa.pt/downloadFile/395139415147/resumo.pdf// (Seen 2015-05-25)

[5] Google Scholar, https://scholar.google.se/

[6] Linköping University Library, https://www.bibl.liu.se/soka/unisearch?l=en/

[7] B. Schneier, *Attack Trees*, Dr. Dobb's Journal, 1999.

[8] T.R Ingoldsby, *Attack Tree-based Threat Risk Analysis*, Amenaza Technologies Limited, 2013.

[9] Z. Yazar, *A Qualitative Risk Analysis and Management Tool - CRAMM*, SANS Institute InfoSec Reading Room, 2002.

[10] I. E. Fray, *A Comparative Study of Risk Assessment Methods, MEHARI & CRAMM with a New Formal Model of Risk Assessment (FoMRA) in Information Systems*, Springer, 2012.

[11] B. Karabacak and I. Sogukpinar, *ISRAM: information security risk analysis method*, Computers & Security, 2005, pp. 147–159.

[12] Software Engineering Institute at Carnegie Mellon University, *OCTAVE* [online] http://www.cert.org/resilience/products-services/octave/ (Seen 2015-05-25)

[13] R.A. Caralli, J.F. Stevens, *Introducing OCTAVE Allegro*, SEI Administrative Agent, 2007.

[14] C & A Security Risk Analysis Group, *Introduction to COBRA* [online] http://www.security-risk-analysis.com/introcob.htm (Seen 2015-05-25)

[15] C & A Systems Security Limited, *ISO 17799 / BS7799 Compliance Checking Made Easy* [online] http://www.riskworld.net/7799.htm (Seen 2015-05-25)

[16] V. Visintine, *An Introduction to Information Risk Assessment*, GSEC Practical, 2003.

[17] C & A Security Risk Analysis Group, *COBRA Risk Consultant* [online] http://www.security-risk-analysis.com/riskcon.htm (Seen 2015-05-25)

[18] C & A Security Risk Analysis Group, *The Risk Assessment Process* [online] http://www.security-risk-analysis.com/cobproc.htm
(Seen 2015-05-25)

[19] A. Toval, J. Nicolas, B. Moros, F. Garcia, *Requirements Reuse for Information Systems Security: A Practitioner's Approach*, Requirements Engineering, 2002.

[20] A. Sylim, Y. Hori, *Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide*, International Conference on Availability, Reliability and Security, 2009.

[21] Club de la securite de l'information Francias, *Mehari 2010*, https://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Overview.pdf
(Seen 2015-05-25)

[22] K. Nagata, Y. Kigawa, D. Cui, *Method to select Effective Risk Mitigation Controls Using Fuzzy Outranking*, Intelligent Systems Design and Applications, 2009, pp. 479-484.

[23] B. Solhaug, K. Stølen, *The CORAS Tool – Downloads* [online] http://coras.sourceforge.net/downloads.html
(Seen 2015-05-25)

[24] B. Solhaug, K. Stølen, *The CORAS Language* [online] http://coras.sourceforge.net/coras_language.html
(Seen 2015-05-25)

[25] F. Braber, I. Hogganvik, M. S. Lund, K. Stølen and F. Vraalsen, *Model-based security analysis in seven steps*, BT Technology Journal, Vol 25 No 1, 2007.

[26] Microsoft, *The STRIDE Threat Model* [online] https://msdn.microsoft.com/en-us/library/ee823878%28v=cs.20%29.aspx
(Seen 2015-05-25)

[27] M. Dekker, *Using attack trees in #cybersecurity for threat and risk modeling* [online] https://www.linkedin.com/pulse/20140529230342-18705719-using-attack-trees-in-cybersecurity-for-threat-and-risk-modeling
(Seen 2015-05-25)

[28] Risk Analysis Consultants, *CRAMM 5 CASE STUDY*, http://www.rac.cz/rac/homepage.nsf/EN/Datasheety
(Seen 2015-05-25)

7 Appendix A - Interview questions

1. Hur skulle du definiera begreppet riskanalys?
2. Använder ni några specifika riskanalysmetoder för att få säkerhet i systemen? - I så fall vilka?
3. Jobbar ni mest med kvalitativa (intuitiva) eller kvantitativa (matematiska) riskanalysmetoder?
4. Tar era riskanalysmetoder hänsyn till ett eller flera problem åt gången?
5. Hur identifierar ni era tillgångar i systemen?
6. Vad är svårast att skydda sig mot?
7. Hur ser riskanalysprocessen ut? - Sker den inför ett specifikt arbete eller är det något som alltid pågår?
8. Anser du att ni lägger stora resurser på att skydda er från hot/göra riskanalyser jämfört med övrig verksamhet? - Vilka typer av resurser (personal/tid/hårdvara/mjukvara)?
9. Vilka jobbar med riskanalys? - Har ni särskilt anställda för detta eller hyr ni in kompetens utifrån?
10. Vad är det viktigaste att fokusera på när man gör riskanalyser?