

UNIVERSITY OF OSLO
Department of informatics

An evaluation of CORAS

Jenny Beate Hougen

Master thesis

1st of August 2006



Abstract

Security is a subject that worries most enterprises. The security threats on distributed systems increases. By using standards for risk management and carry out risk analysis, organisations can improve the quality in their systems and avoid occurrences of potential risks. SINTEF has developed a model-based framework, CORAS, to identify and remedy security risks. The goal of the thesis is to discuss how good CORAS actually is and improve the parts of CORAS.

We present two investigations; one involves a full security analysis of industrial scale using CORAS, the other surveys the need for security standards among organisations.

Acknowledgement

I would like to take this opportunity to express my gratitude to the following that have contributed or helped in realising this thesis.

Writing this thesis has been educational and challenging. I especially want to thank my supervisor Ketil Stølen at SINTEF department of Cooperative and Trusted Systems for contribution with great professional advice and guidance.

This thesis could not have been performed without cooperation with Agresso R&D. A special thank to Tor Gaute Indstøy for believing in me and giving me the opportunity accomplish the security analysis in Agresso. In addition a special thank to Erik Inge Marcussen for supervising me in Agresso.

I also want to thank the analysis team for their patient and excellent teamwork through the analysis. My co-workers in the security analysis were:

Tor Gaute Indstøy
Erik Inge Marcussen
Randi Bjørnbeth
Truls Tveøy
Helge T. Blindheim

Thank you!

I also like to than my father and sister for reading my paper and giving me advice.

Jenny Beate Hougen
Oslo 1st of August 2006

Abbreviations

Agresso:	Agresso R&D
ABW:	Agresso Business World
AGRESSO POF:	AGRESSO PunchOut functionality
CORAS RMP:	CORAS risk management process
MBRA:	Model-based risk analysis

Table of Contents

CHAPTER 1 INTRODUCTION.....	1
1.1 SECURITY ANALYSIS IN GENERAL	2
1.2 THE PROBLEM SCOPE	4
1.3 OVERVIEW OF EVALUATION.....	6
1.3.1 CORAS field trial in Agresso	7
1.3.2 CORAS according to IT-security standards.....	7
1.4 READING GUIDELINE	7
CHAPTER 2 CORAS BACKGROUND	11
2.1 CORAS HISTORY AND GOALS.....	11
2.2 THE CORAS FRAMEWORK.....	12
2.2.1 The CORAS methodology	13
2.2.2 The CORAS library.....	14
2.2.3 The CORAS terminology.....	15
2.3 CORAS DEFINITIONS	15
2.3.1 Security definitions	15
2.3.2 Risk analysis definitions.....	16
2.3.3 IT-security standard definitions.....	18
2.4 A SHORT INTRODUCTION TO THE CORAS RISK MANAGEMENT PROCESS (RMP).....	19
2.4.1 Context identification.....	20
2.4.2 Risk identification	20
2.4.3 Risk estimation.....	21
2.4.4 Risk evaluation.....	21
2.4.5 Risk treatment	22
CHAPTER 3 THE THESIS SUCCESS CRITERIA	23
CHAPTER 4 RESEARCH STRATEGY	25
4.1 RESEARCH METHODS	25
4.1.1 Technology research.....	26
4.1.2 Action research.....	26
4.1.3 Empirical method.....	27
4.2 THE CHOICE OF RESEARCH STRATEGY	28
4.3 CARRYING OUT THE CORAS RESEARCH.....	29
4.3.1 The problem analysis	30
4.3.2 Plan of research.....	31
4.3.3 Accomplish the research.....	32
4.3.4 Evaluation and discussion	36
CHAPTER 5 HYPOTHESES FOR THE EVALUATION OF CORAS	37
5.1 HYPOTHESES WITH RESPECT TO THE CORAS FRAMEWORK.....	37
5.1.1 Hypotheses with respect to the use of the CORAS UML profile	38
5.1.2 Hypotheses with respect to the CORAS tool	40
5.1.3 Hypotheses with respect to the CORAS risk management process	40
5.2 HYPOTHESES WITH RESPECT TO IT-SECURITY STANDARDS	41
CHAPTER 6 CORAS FIELD TRIAL IN AGRESSO	43

6.1	ANALYSIS SUMMARY	44
6.2	USING THE CORAS UML PROFILE	46
6.2.1	<i>The analysis team's view</i>	46
6.2.2	<i>The security analyst's observations</i>	50
6.2.3	<i>Evaluation of the CORAS UML profile</i>	51
6.3	EXPERIENCE WITH THE CORAS TOOL	54
6.3.1	<i>Results from using the CORAS tool</i>	54
6.3.2	<i>Evaluation of the CORAS tool</i>	57
6.4	THE CORAS RISK MANAGEMENT PROCESS.....	59
6.4.1	<i>The analysis team's view</i>	59
6.4.2	<i>Security analyst observations</i>	64
6.4.3	<i>Evaluation of the CORAS risk management process</i>	66
CHAPTER 7 CORAS ACCORDING TO IT-SECURITY STANDARDS.....		69
7.1	SUMMARY OF IT-SECURITY STANDARD INVESTIGATION	69
7.2	RESULTS FROM IT-SECURITY STANDARD INVESTIGATION	70
7.2.1	<i>About the organisations</i>	70
7.2.2	<i>Organisations' opinions on the use of IT-security standards</i>	72
7.2.3	<i>Organisations use of IT-security standards</i>	73
7.3	EVALUATION OF THE IT-SECURITY STANDARD SURVEY RESULTS.....	76
CHAPTER 8 DISCUSSION		81
8.1	THE CORAS FIELD TRIAL IN AGRESSO – A SUCCESS?	81
8.1.1	<i>The CORAS UML profile supports and simplifies the analysis process</i>	82
8.1.2	<i>The CORAS tool increases the quality and efficiency of an analysis</i>	83
8.1.3	<i>Use of the CORAS RMP improves the quality of the organisations' system</i>	85
8.2	THE IT-SECURITY SURVEY INVESTIGATION – A SUCCESS?	87
8.2.1	<i>CORAS is based on the standards most commonly used in practice</i>	87
8.2.2	<i>There is an increasing use and need for IT-security standards</i>	89
CHAPTER 9 FURTHER WORK.....		91
9.1	THE CORAS FRAMEWORK.....	91
9.1.1	<i>The CORAS UML profile</i>	91
9.1.2	<i>The CORAS tool</i>	92
9.1.3	<i>The CORAS risk management process</i>	92
9.2	CORAS ACCORDING TO IT-SECURITY STANDARDS	92
CHAPTER 10 CONCLUSION		95
10.1	SUMMARY.....	95
10.2	RESULTS	96
APPENDIX A	AGRESSO FIELD TRIAL SURVEYS	101
APPENDIX B	IT-SECURITY STANDARD QUESTIONNAIRE.....	107
APPENDIX C	INTRODUCTION TO THE CORAS UML PROFILE.....	110
APPENDIX D	THE AGRESSO SECURITY ANALYSIS REPORT	114

List of Figures

FIGURE 1 AN EAVESDROPPER SNIFFING YOUR BANK LOGIN INFORMATION	1
FIGURE 2 MOTIVATION AND ADVANTAGES OF MODEL-BASED SECURITY ANALYSIS [15]	4
FIGURE 3 EXAMPLE OF THE SYSTEM DEVELOPMENT PROCESS	5
FIGURE 4 CORAS RELATIONS.....	6
FIGURE 5 READING STRUCTURE	8
FIGURE 6 OVERVIEW OF THE CORAS FRAMEWORK	12
FIGURE 7 OVERVIEW THE CORAS METHODOLOGY	13
FIGURE 8 THE CORAS RISK ANALYSIS TOOL.....	14
FIGURE 9 CORAS ELEMENTS.....	17
FIGURE 10 OVERVIEW OF THE CORAS PROCESS	19
FIGURE 11 RELATIONS BETWEEN RESEARCH METHODS AND STRATEGIES	28
FIGURE 12 OVERVIEW OF RESEARCH STRATEGY	30
FIGURE 13 OVERVIEW OF THE FIRST INVESTIGATION	33
FIGURE 14 MILESTONES OF THE FIRST INVESTIGATION	33
FIGURE 15 OVERVIEW OF THE SECOND INVESTIGATION	35
FIGURE 16 MILESTONES DURING THE SECOND INVESTIGATION.....	35
FIGURE 17 COMMUNICATION PROBLEMS	39
FIGURE 18 CAN A MODEL STAND ALONE?	39
FIGURE 19 CHAPTER STRUCTURE.....	44
FIGURE 20 KNOWLEDGE OF TERMS AND CONCEPTS IN A SECURITY ANALYSIS	47
FIGURE 21 PARTICIPANTS UNDERSTANDING OF THE CORAS ELEMENTS	48
FIGURE 22 PARTICIPANTS KNOWLEDGE OF UML	49
FIGURE 23 PARTICIPANTS OPINION ABOUT THE USE OF GRAPHICAL LANGUAGES	49
FIGURE 24 TABLE ERRORS IN THE RISK MATRIX	57
FIGURE 25 THE ANALYSIS TEAM OPINION ABOUT THE TEAM.....	60
FIGURE 26 ANALYSIS TEAM OPINIONS ON THE CONTEXT IDENTIFICATION MEETING.....	62
FIGURE 27 RESULTS OF WHETHER THE ANALYSIS SATISFIED THE TEAMS' EXPECTATIONS	62
FIGURE 28 THE ANALYSIS PARTICIPANTS' OPINION OF THE ANALYSIS EFFICIENCY	63
FIGURE 29 FUTURE USE OF ANALYSIS	64
FIGURE 30 OVERVIEW ORGANISATION SIZE	70
FIGURE 31 OVERVIEW ORGANISATIONS TYPES.....	71
FIGURE 32 OVERVIEW ORGANISATIONS TYPE OF CUSTOMER.....	71
FIGURE 33 OVERVIEW ORGANISATIONS DEGREE OF SOFTWARE DEVELOPMENT	72
FIGURE 34 OPINION ABOUT USE OF STANDARDS 1.....	73
FIGURE 35 OPINION ABOUT USE OF STANDARDS 2.....	73
FIGURE 36 ORGANISATIONS USE OF STANDARDS TO FOLLOW	74
FIGURE 37 PERCENT DEGREE ON ORGANISATIONS FOLLOW/HEARD OF THE STANDARDS.....	75
FIGURE 38 ORGANISATIONS USE OF STANDARDS FOR CERTIFICATION.....	75
FIGURE 39 CERTIFICATION STANDARDS OF WHICH ORGANISATIONS ARE FAMILIAR WITH.....	76

List of Tables

TABLE 1 MAIN ACTIVITIES IN THE CONTEXT IDENTIFICATION SUB-PROCESS	20
TABLE 2 MAIN ACTIVITIES IN THE RISK IDENTIFICATION SUB-PROCESS.....	21
TABLE 3 MAIN ACTIVITIES IN THE RISK ESTIMATION SUB-PROCESS.....	21
TABLE 4 MAIN ACTIVITIES IN THE RISK EVALUATION SUB-PROCESS	21
TABLE 5 MAIN ACTIVITY IN THE RISK TREATMENT PROCESS.....	22
TABLE 6 ROLES AND RESPONSIBILITIES AMONG THE ANALYSIS TEAM	34
TABLE 7 HOW AND WHEN WE COLLECTED EVIDENCE.....	34
TABLE 8 OVERVIEW STANDARDS CORAS IS BASED ON	42
TABLE 9 OVERVIEW ANALYSIS MEETINGS.....	45
TABLE 10 THE INTERVIEWEES' KNOWLEDGE OF TERMS	47
TABLE 11 INTERVIEWEES RESULTS COMPREHENSIBILITY OF THE CORAS ICONS.....	48
TABLE 12 INTERVIEWEE RESULTS OF THE CORAS DIAGRAMS.....	50
TABLE 13 SECURITY ANALYST VIEWPOINT OF THE CORAS UML PROFILE	50
TABLE 14 RESULTS FROM LEARNING THE CORAS TOOL.....	55
TABLE 15 RESULTS FROM USING THE CORAS METHODOLOGY GUIDE.....	55
TABLE 16 RESULTS FROM USING THE TOOLS FUNCTIONALITIES	57
TABLE 17 INTERVIEWEE OPINION OF THE ANALYSIS TEAM.....	60
TABLE 18 QUESTIONNAIRE 2 RESULT ON NUMBER OF PARTICIPANTS IN AN ANALYSIS	61
TABLE 19 INTERVIEWEE OPINION OF THE COMMUNICATION DURING THE MEETINGS.....	61
TABLE 20 INTERVIEWEE OPINION OF THE RISK IDENTIFICATION MEETING	61
TABLE 21 COMMENTS TO FIGURE 27	63
TABLE 22 QUESTIONNAIRE 2 OPINION ABOUT WHAT PART OF DEVELOPMENT PHASE TO PERFORM AN ANALYSIS	63
TABLE 23 COMMENTS TO FIGURE 28	64
TABLE 24 ANALYST OBSERVATIONS ABOUT THE ANALYSIS TEAM	64
TABLE 25 THE ANALYST OBSERVATIONS ABOUT THE ANALYSIS MEETINGS	65
TABLE 26 THE ANALYSIS PROCESS IN GENERAL.....	65
TABLE 27 MISSING OPTION IN QUESTIONNAIRE.....	93
TABLE 28 MAIN RESULT OF THE INVESTIGATIONS.....	97

Chapter 1

Introduction

We become more and more surrounded by systems that help exchanging information and improve the communication between us. You probably use systems to ease your daily work and routines; you may send a couple, maybe a hundred e-mails every day. Perhaps you send e-mails instead of making a phone call, which means that more information is written down and saved. Some of the e-mails written are confidential and could harm you or your organisation if abused. Information is distributed on servers and some of the information should have restricted access. Another example is the use of internet banking to pay bills. You probably do not want anyone to change your bills or payment. To prevent unauthorised access and change of information, access mechanisms such as login with user name and password are used. Organisations perform such types of actions to prevent security breaches. But is this a good enough method to prevent unwanted incidents from happening? What if an eavesdropper listens to the wire between you and your bank (Figure 1) when you logon, and thereby gets your login information and could logon to your account? Then a method that you thought was secure suddenly is not so secure.

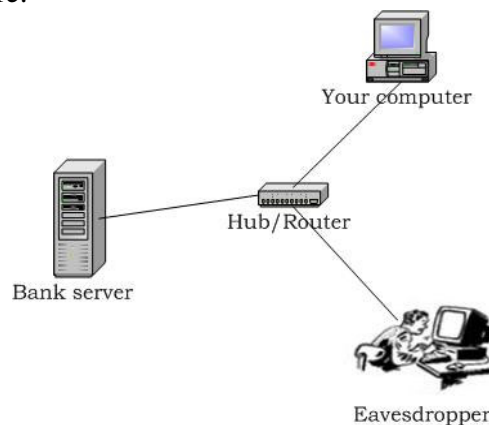


Figure 1 An eavesdropper sniffing your bank login information

In large organisations and systems it is difficult to find all potential risks. The explosive use of internet has increased the transmission of information, but it has also increased the risk of information getting in wrong hands or destroyed. The use of the World Wide Web has created a vulnerable market. Internet-connected computers in homes and companies need protection from intruders. Enterprises are becoming more aware of the need of security and they value the importance of establishing trust and confidence in their products and services. The technology growth increases the need for identifying risks and handling security issues.

There exist several standards, guidelines and methods to manage risk in critical systems and organisations. They can be expensive and time-consuming and several are difficult to learn and understand for non experts. One method for doing risk analysis is CORAS¹. The aim of the CORAS project was to develop a less time consuming and costly method. Simple models the method should be easy to conceive for users as well as developers. This thesis presents an evaluation of CORAS.

This chapter starts by describing security analysis in general; which covers advantages for doing security analyses and constitute the basis motivation for this thesis. The chapter follows with the thesis problem scope and an overall overview of the thesis.

1.1 Security analysis in general

Security analysis is a special form of risk analysis focusing on security risks. It is a technique to identify and assess risks in a system. The goal is to prevent unexpected changes in revenue and costs caused by security issues in an organisation. Organisations perform security analysis of their systems to find potential threats that could harm the system. If the risk found is critical they may invest in actions to prevent those unwanted incidents from happening. An action could be encrypting the communication between the bank and the customer, thereby preventing eavesdroppers from stealing valuable information.

People look at IT-security as a technical aspect, but security is more than technology. To find security risks it is sufficient to look at the technical part of the system. The environmental issues are as well important.

There will now be described the basic procedures of a risk analysis that also applies for a security analysis. A risk analysis should be conducted as part of the business process in an organisation. It would help the organisation to find threats, vulnerabilities, to achieve good design and improve product quality. When performing risk analysis the risk management professionals meet the organisation in order to identify needs and get a common understanding of the target. The risk

¹ CORAS is introduced in Chapter 2

analysis team, compounded by organisation experts and the analysis professional, follows a structured method to identify risks. There exist several available risk analysis methods. Regardless of what method is used, the steps are approximately the same [14]:

1. *Asset identification*: Identify what is of value and relevance in the organisation and in the analysis target.
2. *Risk identification*: Identify threats, risk, concerns and vulnerabilities to the assets found.
3. *Prioritise the risk*: Estimate the risk. Assign consequence and frequency values to the identified risk.
4. *Evaluate risks*: Consider which risks to be treated. The risk level is decided from the consequence and frequency values estimated.
5. *Treat, monitor and control the risks*: Suggest how to treat, monitor or control the risks that were prioritised.

In a risk analysis with focus on security the key elements in each step are confidentiality, integrity and availability. There are many different styles and types of risk analysis, but there are generally two major categories: qualitative and quantitative risk analysis. Qualitative risk analyses do not attempt to assign numeric values to the risk analysis components. Quantitative risk analyses do attempt to assign objective numeric values to the component and to the level of potential losses. [14]

CORAS is a model-based security analysis method. The motivation and advantages for performing model-based security analysis are rendered from [15] and illustrated in Figure 2. In the long-term, correctly and systematically use of model-based security analysis will lead to reduced costs; increasing reuse of documentation will lead to reduce in maintenance cost, early identification of risks will prevent loss of assets value. Use of model-based security analysis will help the design team through the process of building secure and good systems. The use of graphical models will improve the communication between different parts involved and will lead to a correct understanding of the target. Security analyses also have methods that will help teams to prioritise and manage risks and prepare them for the occurrences of unwanted incidents.

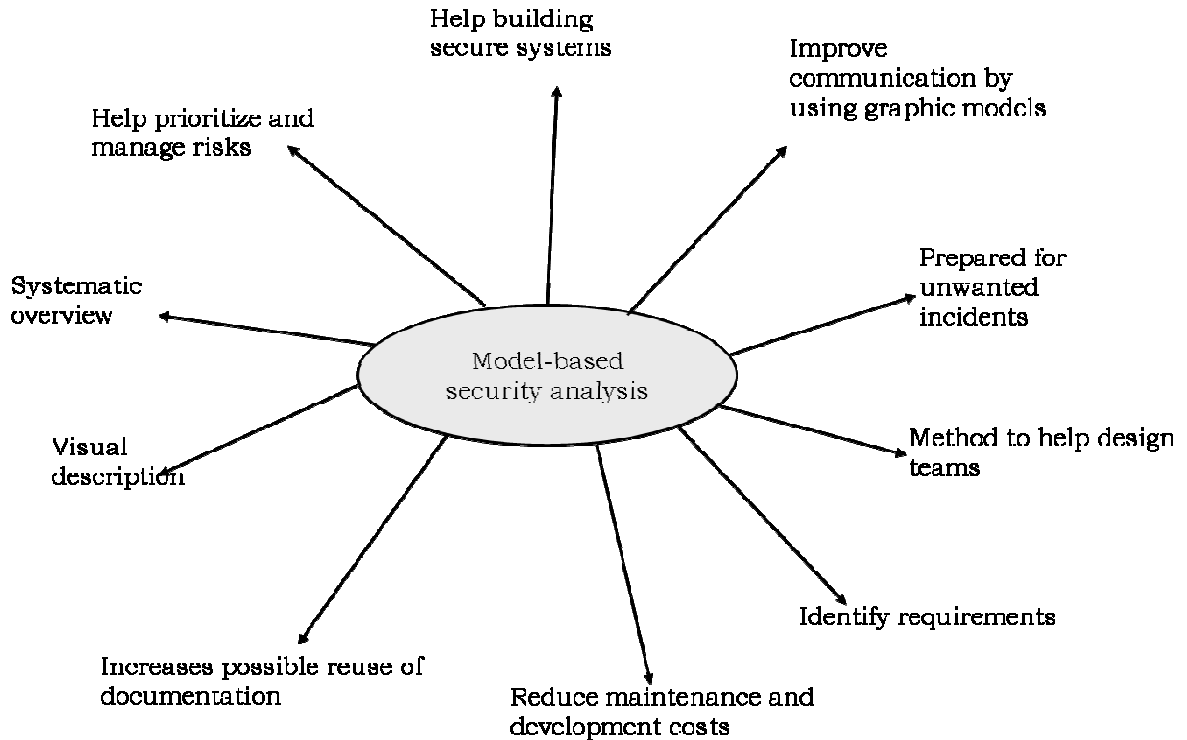


Figure 2 Motivation and advantages of model-based security analysis [15]

1.2 The problem scope

This section discusses some of the issues with CORAS that require research. Some of the questions asked are investigated in this thesis.

The aim of this thesis was to evaluate and improve the CORAS framework for model-based risk analysis (MBRA). The scope of the CORAS framework is wide and there are still problems relating to it that require evaluation and testing. This thesis is part of a long process of evaluating CORAS' usability. CORAS has already been successfully tested in several organisations, but still needs improvement. In order to conclude whether CORAS is a success or not the testing will continue. The research and further development and improvement will carry on after this thesis is finished. The overall goal for the CORAS project is to assess whether CORAS is appropriate for the intended market. One way to do this is to try CORAS out in different organisations and evaluate the result.

CORAS intend to bring the security of systems to a higher level. What level determines if a system is secure or not? There are different opinions about what a secure system is; a security expert desires a system with high security, a customer wants a secure but a usable and functional system. Before performing a security analysis it is important to determine for whom the analysis is carried out, the

analysis viewpoint². The viewpoint decides what direction the rest of the analysis takes. CORAS emphasises the importance of focusing on the analysis viewpoint. The challenge is to make the CORAS customer decide the level of security and the system intention of relevance for the analysis. The main issue is whether CORAS satisfies the customer's security expectations on the desired level of security.

A security analysis could be performed in different phases of the development process. When is it reasonable to perform a security analysis? Focus on security before, during and after the system development process (see Figure 3³). Would it influence the analysis if it was completed in different stages in the development process?

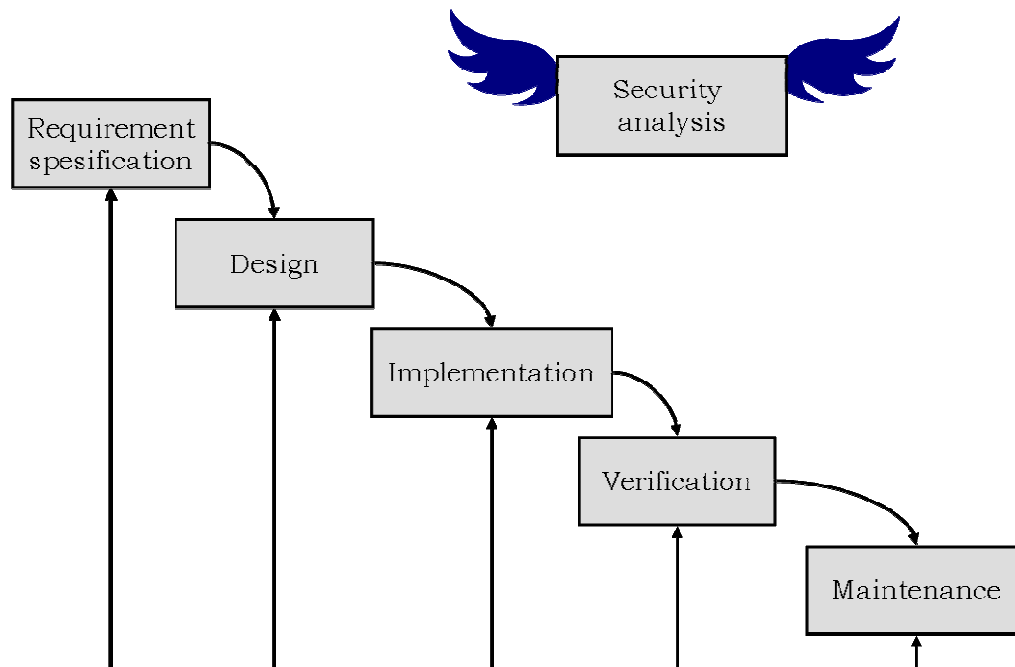


Figure 3 Example of the system development process

An important characteristic of CORAS is the use of models and diagrams. Together with UML (unified modelling language) [5] CORAS uses an own developed graphical language to describe the analysis object. One intention is to improve the communication between the parts in the analysis process. The issue is if these models achieve good target descriptions? Do these models give a satisfying description? How to improve the models? Will the models improve the communication among the team participants?

Assume the research concludes that CORAS works as intended. The results are good and it is proved to be a worthy methodology. This is of course significant, but what if the need for the methodology does not exist? If there is no need for such a methodology, is the research work futile then? This leads to another problem scope;

² A viewpoint could e.g. be the organizations customer or the organization itself.

³ This figure is a typical development process and could not be referred from a particular place.

to find out the need and motivation for IT-security standards among organisations. Is there a need for such methods? Will they be used? Maybe the use of such standards become too expensive.

CORAS is based on several IT-security standards. Are the IT-security standards CORAS is based on the same as the IT-security standards used in practice?

These issues are only a few of what need to be answered before concluding whether CORAS' usability is applicable. This thesis will concern two fields:

- *The CORAS framework:* Try to answer some of the problems of CORAS and thereby improve the framework.
- *CORAS according to IT-security standards:* Investigate if there is a need for such a framework among organisations and if the IT-security standards used are the same as the IT-security standards CORAS is based on.

1.3 Overview of evaluation

The previous section identified the two aspects of CORAS being investigated by this thesis; an evaluation of the CORAS framework and evaluation of the use of IT-security standards among organisations.

To explain the relation between IT-security standards and CORAS an illustration is presented in Figure 4. The intention of CORAS is to offer a good risk analysis method to be used on security critical systems in organisations. The relation between CORAS and IT-security standards is that the CORAS framework is based on known IT-security standards, thus CORAS may have much in common with standards used among organisations.

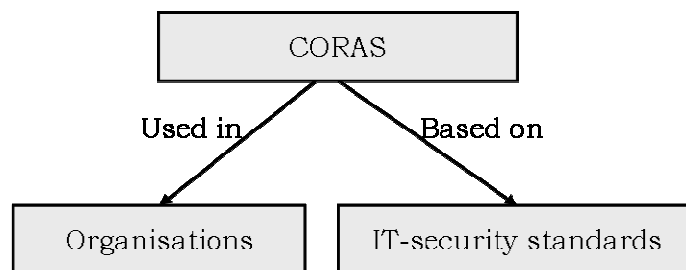


Figure 4 CORAS relations

The work comprises two investigations. In order to evaluate the CORAS framework CORAS was used in an organisation. To evaluate CORAS according to IT-security standards there was performed a survey among different organisations. The following presents an overview of the two areas of evaluation that lead to the result of this thesis.

1.3.1 CORAS field trial in Agresso

The aim of this field trial was to find strengths and weaknesses in the CORAS framework. The framework is large and a complete research will take many years, thus this evaluation only concerns some parts of the framework. The CORAS framework parts investigated were the CORAS UML profile, the CORAS tool and the CORAS risk management process (referred to as CORAS RMP).

In order to investigate the parts of CORAS, CORAS was tested in a real system and. The CORAS RMP was used to perform a risk analysis in this case referred to as security analysis.

The security analysis was performed in the Agresso R&D organisation (referred to as Agresso). Agresso develops a system, Agresso Business World (ABW). The analysis was carried out on a small functionality in ABW, the AGRESSO PunchOut Functionality (AGRESSO POF). This part of ABW is interesting from a security perspective because it reaches out to external systems over the internet.

1.3.2 CORAS according to IT-security standards

CORAS is based on several IT-security standards. By finding organisations use of IT-security standards it would probably cover the need for CORAS. The purpose of the survey was to see if the standards used in practice are the same CORAS is based on, and cover organisations use IT-security standards.

In order to investigate organisations use of IT-security standards there were accomplished a survey among different organisations. A questionnaire was handed out to twenty different organisations. The questionnaire had questions about well-known standards as ISO 27001 (formerly BS 7799) and ISO 17799 and questions about organisations' future use and interest in IT-security standards.

The purpose of investigation was to establish the use of IT-security standards among organisations to declare whether the IT-security standards in use (or used) are the same as the IT-security standards CORAS is based on. Another purpose was to cover organisations intention of using IT-security standards in the future.

1.4 Reading guideline

This section presents the thesis structure. It is meant as a help to the reader and summarises the main points from each chapter and explains the relations of the chapter. Figure 5 gives a graphical presentation of the structure.

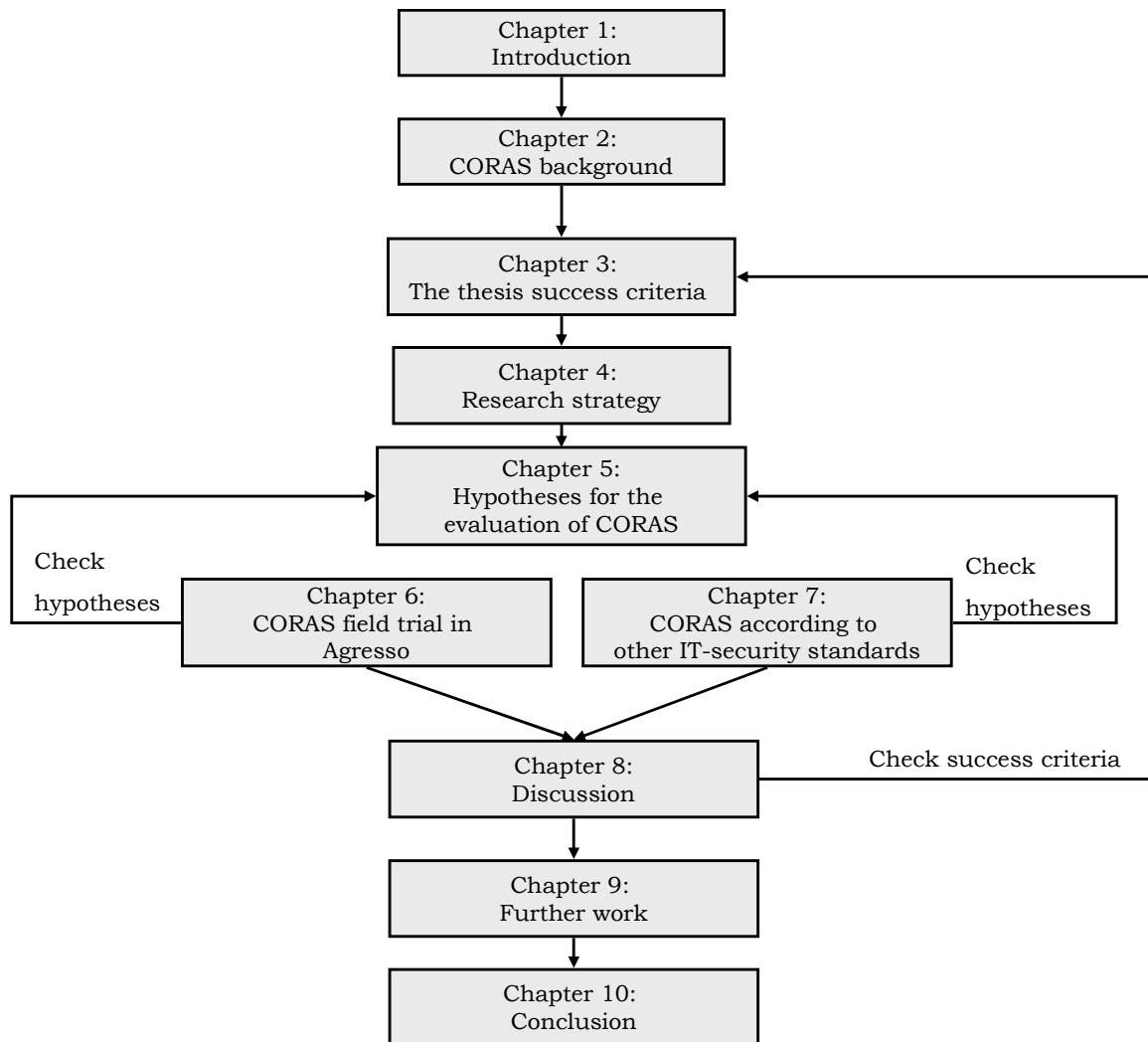


Figure 5 Reading structure

CHAPTER 1 *Introduction*: Establishes and motivates the research purpose. It explains the security analysis concept, describes the problem scope and presents the research performed that constitutes the basis of the evaluation.

CHAPTER 2 *CORAS background*: Gives an introduction to CORAS. It provides background information of CORAS, including the overall CORAS framework, history and goals and the CORAS risk management process.

CHAPTER 3 *The thesis success criteria*: This chapter presents the thesis success criteria that used in Chapter 8 to discuss the evaluation of the result in Chapter 6 and Chapter 7. The goal of the thesis is to answer these success criteria.

CHAPTER 4 *The Research strategy*: Provides a description of the research strategy followed during the study. The chapter gives an explanation of well–

known research methods and strategies that creates the background for the choice of research strategy.

CHAPTER 5: *Hypotheses for the evaluation of CORAS*: Formulates the hypotheses used for evaluation of the results (in Chapter 6 and Chapter 7) gathered during research.

CHAPTER 6 *CORAS field trial in Agresso*: Presents the results acquired during the security analysis performed in Agresso. The results are evaluated according to the hypotheses defined in Chapter 5.1. The analysis report is given in Appendix D.

CHAPTER 7 *CORAS according to other IT-security standards*: Gives the result of twenty different organisations' answers to questionnaires handed out. The results are evaluated with the hypotheses in Chapter 5.2.

CHAPTER 8 *Discussion*: Based on the thesis success criteria in Chapter 3 it discusses whether the aim of the thesis is achieved. An appreciation of the evaluation performed in Chapter 6 and Chapter 7 are considered.

CHAPTER 9 *Further work*: Modifications are suggested and work is recommended in order to continue the research.

CHAPTER 10 *Conclusion*: Summarises and concludes the accomplishment and findings.

APPENDIX A: Contains the questionnaires and interview used in the Agresso field trial.

APPENDIX B: Contains the questionnaire used for the IT-security standard investigation.

APPENDIX C: Introduce the CORAS UML profile.

APPENDIX D: Presents the security analysis report. For security reasons some of the risks and information has been removed or hidden behind black boxes.

Chapter 2

CORAS Background

CORAS is a method for doing risk assessment of security-critical systems. The purpose of CORAS is to help integrate security into system development. One of the main objectives of CORAS is to develop a practical framework to support and simplify risk management. The framework includes an experience library from previous projects, the methodology for doing risk assessment and a terminology to use in the projects.

The purpose of this chapter is to give the reader enough background information to understand the framework. Unless otherwise stated the information is restated from [1].

2.1 CORAS history and goals

The CORAS project started in January 2001, and in September 2003 the first version of the framework results was released. The EU-funded project CORAS was terminated in 2003 and is now a part of the SECURIS project. The first version was created in an EU- project. The CORAS consortium consisted of eleven institutions from European countries. The later versions have been developed by SINTEF among other projects like SECURIS [6], TrustCoM, ENFORCE [4]. At present SINTEF is in charge of the development of CORAS.

During the past years CORAS has been tried out on different organisations. The result of these field trials has been evaluated and used to improve the framework. It has been tested in telemedicine and e-commerce systems with success.

The main goal of CORAS is to create a model-based methodology that is able to detect all types of risks in an environment, an improved method for precise, unambiguous and efficient risk analysis of security critical IT systems. The use of

models will give a structured overview of the system and detect more risks. The goal is to use models comprehensible for all parts involved.

The aim of developing CORAS was to establish a method to maintain security in systems and to create a cost-effective risk assessment process. Not only the technical security has been emphasized; the organisational and business context was equally important [4]. When organisations worry about security, they tend to focus primarily on the technical security issues. Several organisations are not aware of the frequently security breaches caused by the organisations environment⁴. Hence there is a need for building structured methods to handle both technical and organisations environmental security issues. CORAS covers both technical and organisations environmental vulnerabilities.

2.2 The CORAS framework

This chapter describes the results of CORAS. The CORAS framework is based on the Reference Model for Open Distributing Processing (RM-ODP) [20]. RM-ODP has an object-oriented foundation and defines concepts and structuring rules for describing the architecture of distributed systems.

The framework (Figure 6) gives the overall structure of the CORAS three main results. It supports the risk analysis team when doing the risk analysis by providing a terminology, a methodology and a library to use. The use of the CORAS framework is a complex process that involves both humans and tools [3]. Therefore, a tool has been developed to support the framework.

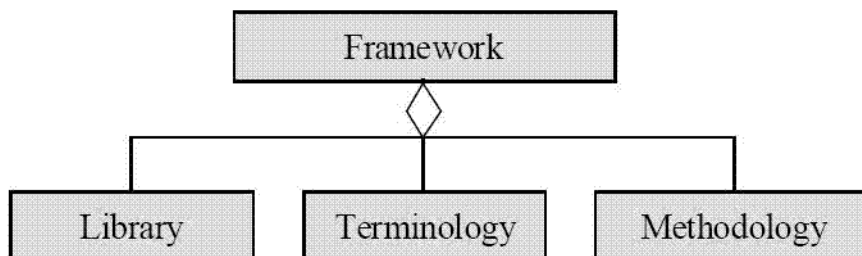


Figure 6 Overview of the CORAS framework

The following sections explain the three results of the CORAS framework and the results role in an analysis process.

⁴ Security breaches caused by the environment could be human threats e.g. an employee leaving the door to the organisation open or writes down the password on his computer.

2.2.1 The CORAS methodology

The methodology consists of a tool, guidelines for doing the risk management and languages used to support the different activities in the risk management process. An overview of the methodology result is given in Figure 7.

The MBRA methodology involves a platform for tool integration, a risk management process (introduced in Section 2.4) and a system development process (CORAS IRM-SDP, integrated risk management and system development process), and languages (XML, UML etc.) for representing security assessment information.

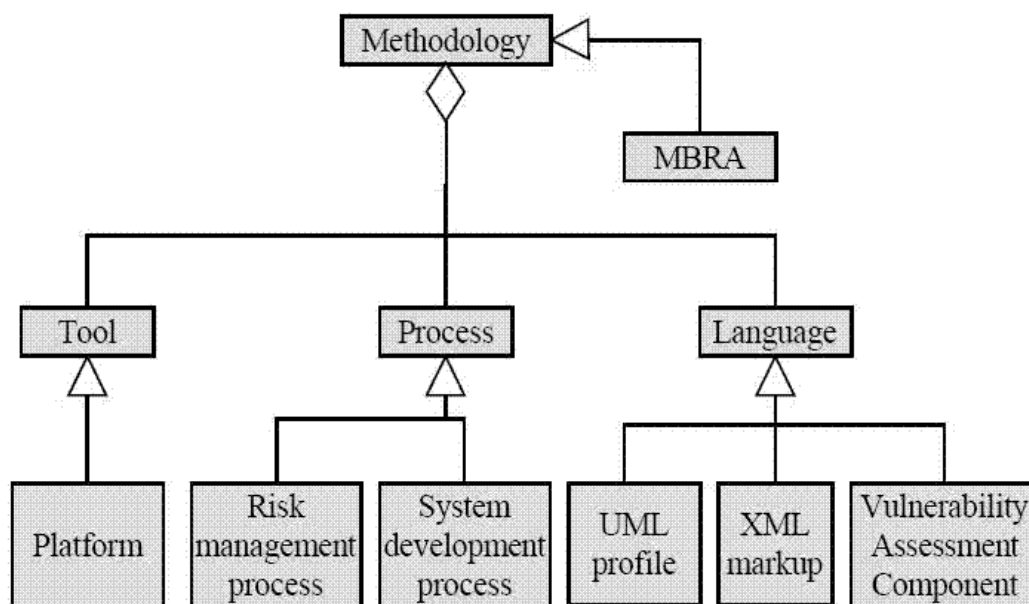


Figure 7 Overview the CORAS methodology

As mentioned the CORAS framework is provided with an integrated tool. The tool is used to simplify and easily document the analysis process. It is an open source product and can be downloaded from <http://coras.sourceforge.net>. In the current version of CORAS, there is both a web based tool and a desktop-based tool. In Figure 8 shows the desktop-based tool, consisting of:

- A library of reusable experience packages
- The risk analysis project engaged
- A tutorial of the CORAS methodology with description of the tools function.

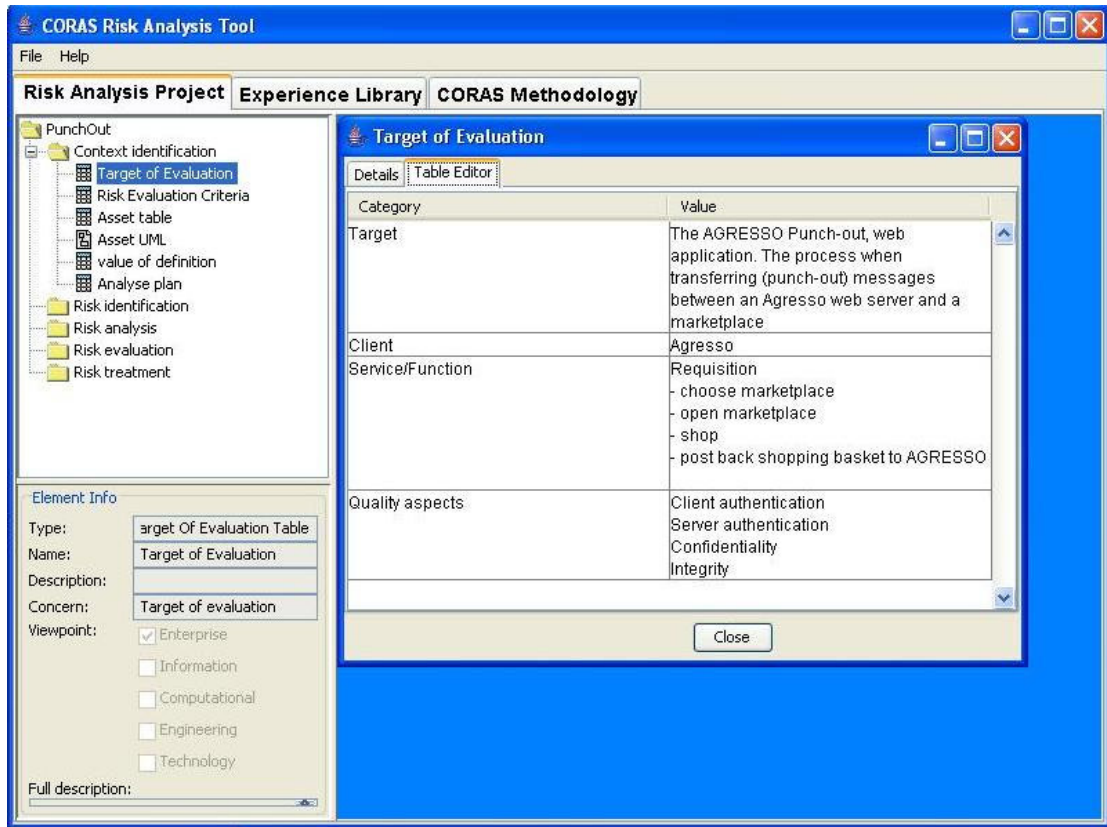


Figure 8 The CORAS risk analysis tool

The language supports the risk analysis process. CORAS suggest using known languages (e.g. UML and XML). In addition, a CORAS' specific graphical language has been devised. The CORAS graphical language is explained in more detailed in Appendix C.

The intention of a graphical language is to facilitate communication and interaction between different groups of stakeholders involved in a security assessment. The focuses of CORAS are good documentation, analysis, maintenance and reporting. It is believed that the use of such graphical language with belonging description creates good documentation.

There are three important purposes to use models when doing a risk assessment:

- Describe the target of evaluation at the right level of abstraction
- To simplify the communication between the different participants involved
- Document the risk assessment result to support reuse and maintenance

2.2.2 The CORAS library

During a risk analysis there will be several risks identified. These risks may have been identified in earlier cases or there could be risks that have much in common. To avoid doing the same process a number of times, one will probably save a lot of work by storing the analysis results in a library. It saves time and avoids mistakes

and erroneous decisions. The CORAS reusable elements repository (RER) is designed to facilitate reuse of experiences from risk assessments. The library is among other based on standards such as UML, XML and XSL.

There are two libraries in the CORAS framework:

- *The experience library*: Supports the risk assessment process by providing general reusable elements.
- *The assessment library*: Stores elements from actual risk assessment.

The libraries are used by the risk analysis team to assist in the risk assessment process. The advantage of the libraries is firstly to the facilities of reuse (the user avoids starting from scratch), secondly to document the risk assessment.

2.2.3 The CORAS terminology

The terminology defines central terms and their relationships in the framework. The CORAS terminology is divided into three parts; security terminology (related to IT-security), RM-ODP terminology and risk analysis terminology. The concepts of security and risk analysis are taken from several international standards like AS/NZS 4360 (the remaining standards are listed in Table 8). Some of the terms are defined in the next section (2.3). The purpose of defining terminology is to clarify confusing or misunderstood terms among participants in a security analysis.

2.3 CORAS definitions

This section presents relevant security and risk terms. The definitions are a part of the CORAS framework as described in section 2.2. Only terms necessary for this thesis will be defined.

2.3.1 Security definitions

This section presents the general security terms defined in the CORAS terminology.

- *IT-security*: All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability.
- *Availability*: The property of being accessible and usable upon demand by an authorised entity.
- *Confidentiality*: The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

- *Data Integrity*: The property that data has not been altered or destroyed in an unauthorised manner.
- *Non-repudiation*: The ability to prove an action or event has taken place, so that this event or action cannot be repudiated later. (In message based communication protocols non-repudiation provides proof of expedition or receipt, so that it shall be impossible to falsely claim not having sent or received a digital message.) (In general non repudiation can be seen as a special case of accountability).
- *Accountability*: The property that ensures that the actions of an entity may be traced uniquely to the entity.
- *Authenticity*: The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.
- *Reliability*: The property of consistent intended behaviour and results.

2.3.2 Risk analysis definitions

This section presents risk analysis terms used during a risk management process with CORAS. The terms are taken from the CORAS terminology.

- *Assets*: Something to which an organisation directly assigns value and, hence, for which the organisation requires protection.
- *Consequence*: The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event
- *Frequency*: A measure of the rate of occurrence of an event expressed as the number of occurrences of an event in a given time. See also Likelihood and Probability.
- *HazOp (Hazard and operability study)*: A technique for identifying and analysing the hazards and operational concerns of a system [11].
- *Risk*: The chance of something happening that will have an impact upon objectives. It is measured in terms of consequence and likelihood.
- *Risk Analysis*: A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
- *Risk Assessment*: The overall process of risk analysis and risk evaluation.
- *Risk Identification*: The process of determining what can happen, why and how.
- *Risk Management*: The culture, processes and structures that are directed towards effective management of potential opportunities and adverse effects.
- *Risk Management Process*: The systematic application of management policies, procedures a practice to the tasks of establishing the context, identifying, and analysing, evaluating, treating, monitoring and communicating risk.
- *Risk Treatment*: Selection and implementation of appropriate options for dealing with risk.

- *Stakeholders*: Those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity.
- *Target of Evaluation (TOE)*: an IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation
- *Threat identification*: Valuable information on potential threats can be gathered by the review of attack-alerts logged by intrusion detection tools. These logs provide a source of information on security incidents that posed a threat to the system security in the past.
- *Unwanted incident*: incident such as loss of confidentiality, integrity and/or availability.
- *Vulnerability identification*: The main results of vulnerability assessment tools are the identification of the known vulnerabilities associated to the current versions of the operating systems and services.

Figure 9 shows a graphical overview of the elements and terms used in CORAS.

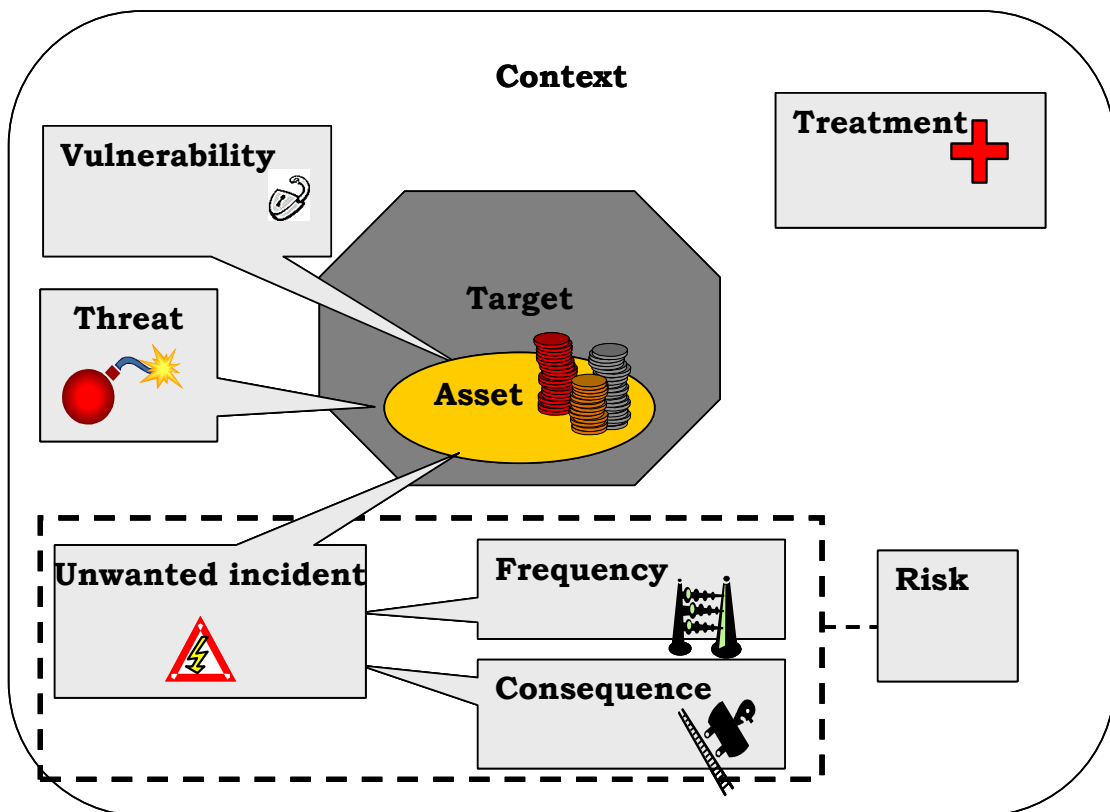


Figure 9 CORAS elements

2.3.3 IT-security standard definitions

CORAS is based on several IT-security and risk management standards. Below defines the IT-security standards CORAS is based on.

- *AS/NZS 4360*: Australian / New Zealand Standard for Risk Management. This Standard provides a generic guide for managing risk [16]
- *ISO 13335*: IT security management – comprises a set of guidelines for the management of IT security, focusing primarily on technical security control measures [17]
- *ISO 17799 (ISO 27001)*: This is the Code of Practice describing a comprehensive set of information security control objectives and outlines a menu of best-practice security controls [18]
- *IEC 61508*: Is the international standard for electrical, electronic and programmable electronic safety related systems. It sets out the requirements for ensuring that systems are designed, implemented, operated and maintained to provide the required safety integrity level (SIL) [19]

2.4 A short introduction to the CORAS risk management process (RMP)

To find potential threats in a system the CORAS risk management process defines five sub-processes. The five sub-processes each have several activities. As stated in Figure 10, each step could be reviewed if necessary. It is important that the analysis team communicate and consult during the sub-processes.

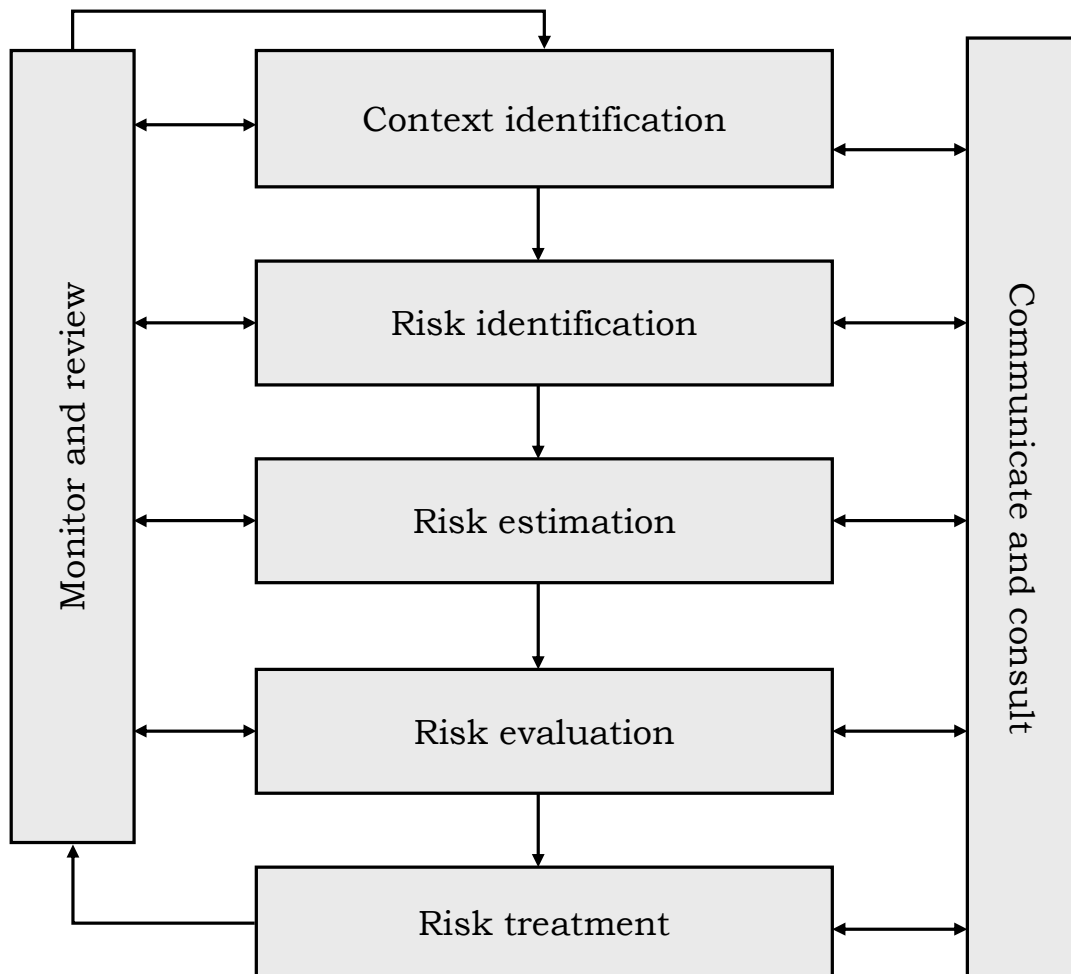


Figure 10 Overview of the CORAS process

It is not mandatory to follow the full guideline. It is up to the risk analyst leader to decide the necessary activities to follow. This section gives a short tutorial on the process of a security analysis based on the CORAS methodology. The information is gathered from the CORAS platform tool.

2.4.1 Context identification

The goal of the context identification process is to establish an understanding of what to evaluate. It is important to find the stakeholders⁵ motive and goal with the analysis. What do the stakeholders want to protect? The context identification process sets the stage for the rest of the process. It is important to understand the exact target of analysis, in order to find potential risks. Table 1 gives the activities to do in order to achieve the intention of this sub-process.

Activity	Description
Identify areas of relevance	Provide a correct and complete description of the target of evaluation and its related areas of relevance. It is divided into five sub-activities; risk management context, organisational context, SWOT analysis, documentation and target of evaluation.
Identify and value assets	Identify the assets relevant to the target of evaluation. The assets make the focus for the rest of the analysis.
Identify risk evaluation criteria	Give an estimate of the loss in assets a client can tolerate over a given time.
Approval	Ensure that the documentation from the previous steps is correct and complete.

Table 1 Main activities in the context identification sub-process

2.4.2 Risk identification

This activity suggests methods to identify potential threats and vulnerabilities pursuant to the analysis target described in the context identification. The threats and vulnerabilities may be found through structured brainstorming methods (e.g. Hazard and operability analysis) and questionnaires. The process involves a team of security experts, system owners, system developers and risk analysis experts. The risk identification process consists of three activities explained in Table 2.

Activity	Description
Identify threats to assets	Makes use of selected techniques and fragments from conventional risk analysis methods. Use these methods to identify which threats that could lead to loss in the assets (the assets found in the context identification sub-process).

⁵ It could be one or several stakeholders attach to an analysis

Activity	Description
Identify vulnerabilities of assets	Identify vulnerabilities of assets by using questionnaires.
Document unwanted incidents	Combine and structure the results from previous steps and decide whether further threats or vulnerabilities identifications are needed.

Table 2 Main activities in the risk identification sub-process

2.4.3 Risk estimation

This sub-process estimates the risk found in the risk identification sub-process. The analysis team assigns the risks consequences and frequency values. The sub-process is divided into three activities explained in Table 3.

Activity	Description
Consequence evaluation	Analyse, evaluate and document the consequences of the unwanted incidents.
Frequency evaluation	Come up with realistic estimates for the probabilities that for each specific unwanted incident to occur.
Determine level of risk estimation	For each unwanted incident to combine the consequence value and frequency value into an estimate for the level of the risk.

Table 3 Main activities in the risk estimation sub-process

2.4.4 Risk evaluation

This sub-process evaluates the risks to find what risks that need treatment. The sub-activities are explained in Table 4.

Activity	Description
Prioritise risks	Priorities each risk. Decide whether the risk should be accepted or not and sort the risk by priority.
Classify risks into categories	Identify the risk categories to be applied and document them. Assign the risk that has not been accepted to its appropriate category.
Prioritise the risk categories	Assign the risk category values. For each risk theme calculate an overall risk value and assign a risk category priority. Document the result in a risk value table.

Table 4 Main activities in the risk evaluation sub-process

2.4.5 Risk treatment

The last sub-process is the risk treatment. Based on the evaluation done in the previous activity there were suggest treatment to the risk that was decided to treat. The activities of this step are explained in Table 5.

Activity	Description
Identify treatment options	Assign one or several treatment options for each risk category and document and illustrate the treatment options.
Assess alternative treatment approaches	Do a cost and benefit analysis and prioritise for each treatment option.

Table 5 Main activity in the risk treatment process

Chapter 3

The thesis success criteria

The purpose of this thesis was to further investigate the CORAS framework in order to improve the different parts of the framework such as the tool, the CORAS UML profile and CORAS RMP. The approach was to bring the research of CORAS to the next level. The expectation was to be able to accomplish an analysis in an organisation, and perform a survey among organisations to state the organisations need and use of IT-security standards.

In order to limit the research thesis success criteria were established. The goal of this thesis is to be able to answer the thesis success criteria. To further answer the success criteria there were established hypotheses in each investigation part (given in Chapter 5).

The thesis success criteria are the superior hypotheses based on the evaluation of the CORAS's framework and CORAS according to IT-security standards. The success criteria are used for discussion in Chapter 8 and are used to evaluate whether this research validate the hypotheses.

THE THESIS SUCCESS CRITERIA:

- The field trial in Agresso is successful if we are able to evaluate CORAS with respect to whether:
 - The CORAS UML profile supports and simplifies the analysis process
 - The CORAS tool increases the quality and efficiency of an analysis
 - Use of the CORAS RMP improves the quality of the organisations' system
- The IT-security standard survey is successful if we are able to evaluate whether:
 - CORAS is based on the standards most commonly used in practice
 - There is an increasing use and need for IT-security standards

Chapter 4

Research strategy

This chapter motivates and present the thesis research strategy. It describes the research progress from beginning to end; how the research strategy was chosen, planning of the research and collecting results.

The aim of research is arrive at something new, either a new theory or a new artefact. When doing research, the goal is to produce a solution to an unsolved problem. It is common to distinguish between two types of research, classic research and technology research. The classic research tries to find a solution to a problem related to the structure of the real world. Technology research is research trying to construct new and better artefacts (human created entities). In both cases, hypotheses are either verified or falsified. The hypotheses evaluation may result in a new design which is checked against the specification of the artefact to evaluate the quality.

Since this thesis was concerned with evaluating and recommending improvements to an artefact (CORAS), the thesis belongs to the area of technology research.

When performing technology research several research strategies are available. Each strategy has different strengths and weaknesses.

Section 4.1 introduces the basic research strategies and methods available which establish a basis for the choice of research strategy. Section 4.2 present an overview of the choice and Section 4.3 describes how the research was performed. Unless otherwise stated the information about research methods is gathered from [9].

4.1 Research methods

A research method is a method for developing and finding the evidence of research hypotheses. The difference between strategy and method may be confusing; a

research strategy is a description of the entire process of finding an answer to the research problem, a recipe on how to complete our research. A method could be a step in the process of finding those answers. Several methods can be used during the research strategy. There are several different research methods, and it is not always easy to distinguish between them.

The following section is present the methods that constitute the basis for our choice of research strategy.

4.1.1 Technology research

Technology research is about constructing new and better artefacts. With technology research, you carry out a problem analysis and a specification of the artefact. Next, you create a new design of the artefact specification. Then you find evidence to back up your design. The purpose of technology research is to find out if the design satisfies the specification.

4.1.2 Action research

There are different forms of action research. Since the mid-twentieth century, the action research has been used in social and medical science. Now the method is also used in the science of information systems. The researchers' task is to analyse both the subjects (e.g. elements in an environment) and the social situation in the research environments.

Action research has its root in social and psychological science. Hence, it is important to understand the complexity of social organisation in the problem. The researcher and the client operate together. The goal of the researcher and the client must not deviate significantly. An action researcher will as part of the research not just observe, but be actively involved within the research. This way of working will provide benefits for both the researcher and the organisation.

The action research approach is to implement change and study the changes. A key assumption of the action researcher is that the result of splitting the organisation and the technology into smaller pieces will not lead to useful information about the situation.

One form of action research, known as the "participatory action research", is the five-step model [10]. It requires the establishment of a client-system infrastructure or a research environment. This is the environment where the researcher has authority or sanction to specify actions. It includes boundaries of the research domain, the entries and exits of the scientists. The five phases are:

1. *Diagnosing*: Identifying the primary problems that are the underlying causes of the organisation's desire for change.
2. *Action planning*: Specification of organisational actions that should relieve or improve these primary problems. These planned actions are about discovering some desired future state for the organisation and the changes that would achieve such a state.
3. *Action taking*: Implement the planned actions. The researcher and the practitioners collaborate.
4. *Evaluating*: Evaluating the outcome of the completed actions. Where the change was successful, the evaluation must critically question, what is the reason for success? If the change was unsuccessful, it should be established a framework (make change to elicit a better result) for the next iteration of the action research cycle.
5. *Specifying learning*: The last phase is to specify the knowledge gained during the process. It is about learning something for further use in research.

The five phases may be cycled. Not only if it was a success, but also to develop further knowledge about the organisation and the validity of relevant theoretical frameworks. [10]

4.1.3 Empirical method

The four research methods used in software engineering are the scientific method, the engineering method, the empirical method and the analytical method [1]. A closer look at empirical method is now presented.

Empirical method is based on empirical studies. As for action research, the empirical studies come from social science and psychology. In these studies, human behaviour is of importance. Software engineering has non-formal rules and laws because of human behaviour and it cannot expect to find any formal rules because people develop the software. Empirical methods include the investigation techniques survey, case study and experiments.

Survey is an investigation technique that primary uses interviews and questionnaires to gather information. Surveys are used before a tool is used or when a tool has been used for a while. It could be appropriate to use surveys to study how a new development process has improved the developers' attitude towards quality assurance. For example when we are interested in finding out what people think about a tool/product. The purpose is to understand the opinions of the population. What is the general opinion of the product? The objectives when conducting surveys are descriptive, explanatory and explorative [9].

Case studies are studies observing or monitoring projects, activities or assignments. With case studies, we are investigating an entity or phenomenon for a period. When doing case studies we are looking at the changes with respect to an existing design

or a specification, to see the differences. It is appropriate when finding out which entity is best or evaluating the differences between two methods. It can be viewed as a comparative research strategy, by comparing one method in one approach with the same method used in another approach [6].

Experiments are normally done in a laboratory environment. While doing experiments the variables are manipulated and controlled. The difference in experiments and case studies are that in experiments the situation is controlled by manipulating state variables, but in case studies changes are applied and the effects are observed. Experiments are appropriate in various situations i.e. testing whether the accuracy of certain models is as expected, testing existing theories, testing people conceptions, exploring relationships, and validating measures [9].

Carrying out experiments involves different steps as definition, planning, operation, analysis, interpretation, presentation and package [9].

4.2 The choice of research strategy

When doing research we need a strategy for how to proceed. The following explain the relations between the methods and strategies used in the thesis research.

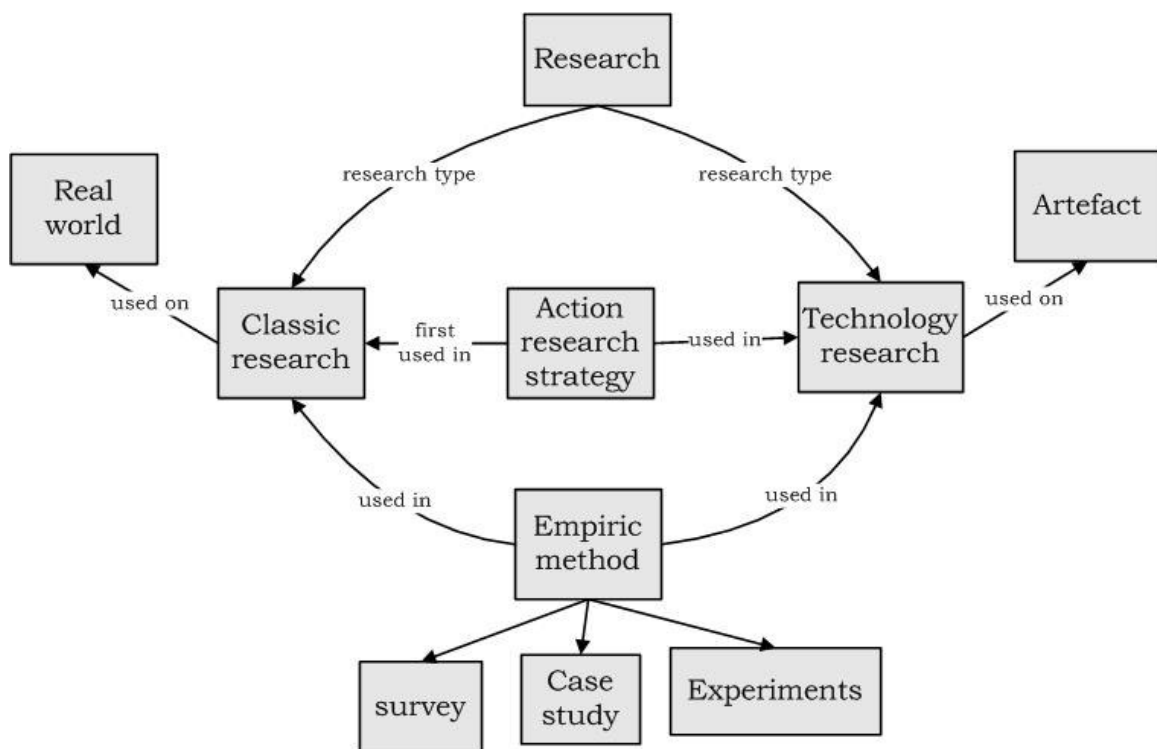


Figure 11 Relations between research methods and strategies

This study is dealing with an artefact (CORAS) which means that it falls into the category technology research. As illustrated in Figure 11 action research has its root

in classic research because it was first used in social and medical science (researches in the real world). Because of its focus in humans, their behaviour and the close collaboration between humans, it is still related to classic research. In action research the researcher will be actively involved in the research object. During this research there we were not actively involved in CORAS, thus this was not action research. The research strategy inherits some ideas from action research because there were followed some of the phases described in Section 4.1.2.

The empiric methods are frequently used in both technology research and classical research. This requires specific methods and techniques to collect results.

4.3 Carrying out the CORAS research

This section describes the thesis research process. The use of empiric methods was chosen. The introduction chapter presented two investigations of evaluation, the evaluation of the parts in the CORAS framework and the CORAS according to IT-security standards. Below is a presentation of how the research of these two areas was accomplished.

An overview of the research strategy is in Figure 12. The figure presents the relation between the research phases. The four phases are:

1. *Problem analysis:* The problem analysis specifies the research of CORAS which includes; the two research investigations, the decided research methods to use, and the formulated hypotheses. The hypotheses were categorised into hypotheses related to the CORAS framework (Section 5.1) and hypotheses related to CORAS according to IT-security standards (Section 5.2).
2. *Plan of research:* This phase planned the accomplishment of the research. The planning implied deciding how to test the hypotheses formulated in the problem analysis and how to gather evidences (results). In order to collect necessary results two investigations were planned; Using CORAS in an organisation, and perform an IT-security standard survey among organisation.
3. *Accomplish the research:* In this phase the planned investigations were accomplished. Evidences were collected during the accomplishment of both investigations.
4. *Evaluate the results:* This phase compared the results collected from the investigations to the hypotheses stated during the problem analysis.

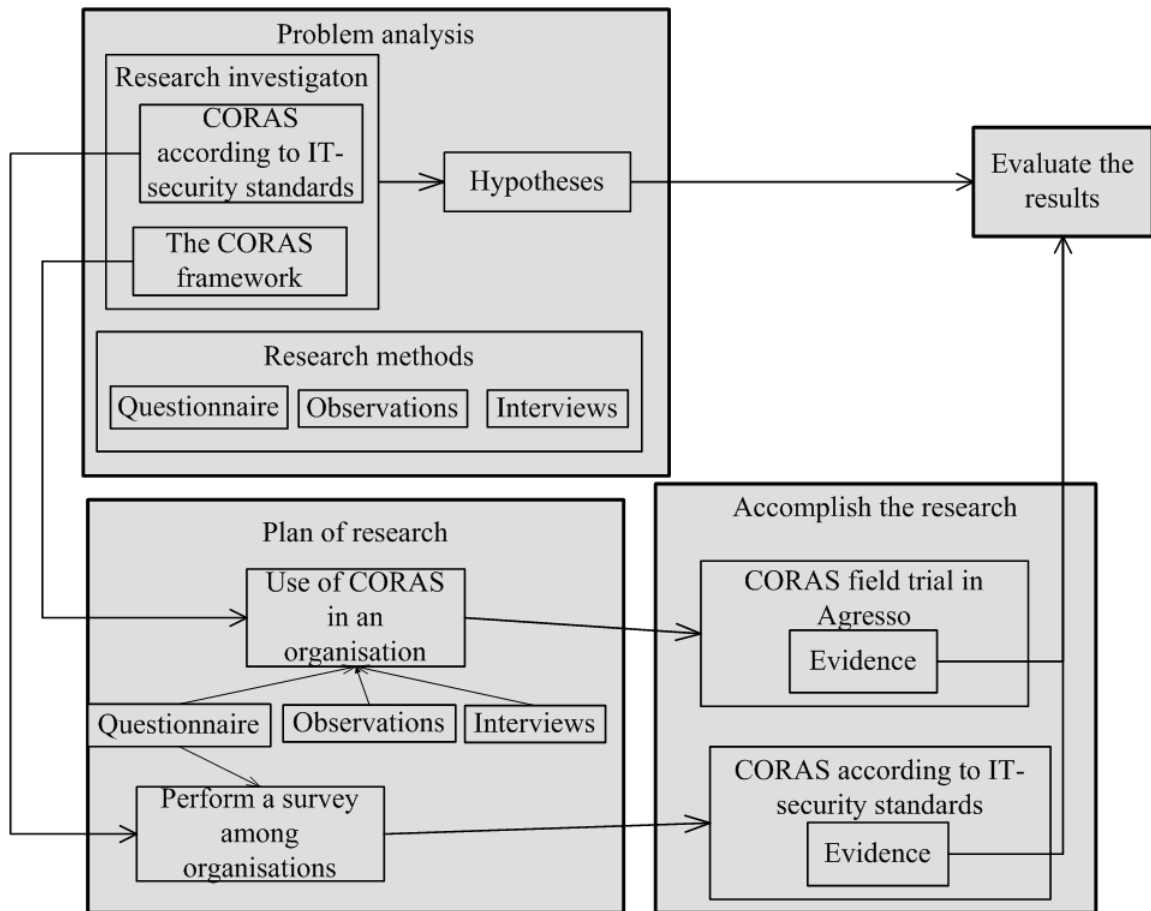


Figure 12 Overview of research strategy

The following gives a more detailed description of each research phase.

4.3.1 The problem analysis

The research started by creating the problem analysis. This section presents the research investigation, the research technique and the research methods from the problem analysis.

4.3.1.1 The research investigation

The first step of this research was to define what to investigate within CORAS. What need change? What do we want to achieve with the research?

The goal of this analysis was to continue the CORAS research and find possible weaknesses with the design that require change. Based on the CORAS requirement specification [8] it was decided to investigate three parts of the CORAS framework. Another point of interest that required investigation was finding out organisations need for CORAS. CORAS is based on well known IT-security standards. Thus to

investigate the organisations knowledge of IT-security standards and their use of such standards if relevant would be useful.

The problem analysis resulted in two research investigations:

- *The CORAS framework*: The CORAS framework needed testing and improvement. The parts of the framework was:
 - The CORAS UML profile
 - The CORAS risk management process
 - The CORAS risk analysis tool
- *CORAS according to IT-security standards*: To find out about the use of IT-security standards among organisations in order to answer some questions about CORAS:
 - Do organisations need CORAS?
 - Is CORAS based on the same standards as those used in practice?

4.3.1.2 Evaluation technique

The previous section defined what research investigation parts to evaluate. For both of the investigations a number of hypotheses were formulated. The purpose of formulating hypotheses was to investigate them empirically. The hypotheses are given in Chapter 5.

4.3.1.3 Research methods

There exist several investigation techniques on how to collect evidence during research. The following were chosen:

- *Observations*: Through experience and observations the analyst leader collected results from learning the methodology and the tool, using the UML profile and from the analysis process itself.
- *Questionnaires*: Data were collected from the analysis team. There two questionnaires were completed among the team.
- *Interviews*: During the analysis, interviews were performed among some of the team members.

The results are presented in Chapter 6 and Chapter 7.

4.3.2 Plan of research

The problem analysis defined the research investigation, the evaluation technique to use and research methods used when collecting evidence. The next phase in the research was to plan how results collection should be accomplished. Based on the two research investigations, two investigations were planned:

- *Use of CORAS in an organisation:* In order to investigate the parts of CORAS's framework the plan was to use the parts of the framework in an organisation. Questionnaire, interviews and observations were used during the investigation.
- *Perform a survey among organisations:* The purpose of this investigation was to map organisations use and need of IT-security standards. Questionnaire was handed out to several organisations.

4.3.3 Accomplish the research

In order to accomplish the plan it required one organisation willing to perform a security analysis and several organisations to answer the IT-security standard survey. Below is a presentation of how the two investigations were completed.

4.3.3.1 First investigation: CORAS field trial in Agresso

The purpose of this field trial was to answer some of the problems with the CORAS UML profile, the CORAS RMP and the CORAS tool. In order to investigate these parts of the framework the CORAS RMP was used to execute a security analysis in the Agresso organisation. The analysis focused on a small functionality in their system, the AGRESSO POF.

An overview of the field trial is given in Figure 13. The CORAS RMP included use of the CORAS UML profile and use the CORAS tool to store the results and as a guide during the process. The analysis closed with generating an analysis report. Evidences were collected by gather information form the analysis participants, and trough the analysts observations and monitoring of the different parts in the analysis. Finally all the evidences were evaluated and concluded.

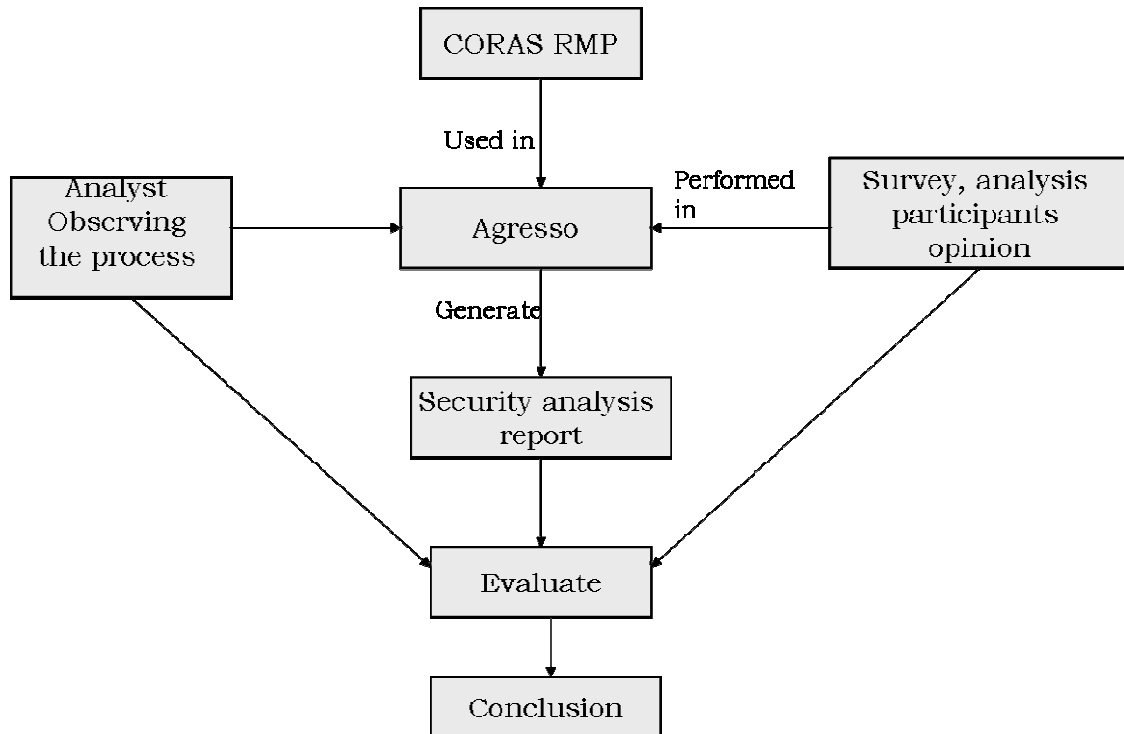


Figure 13 Overview of the first investigation

Figure 14 displays milestones for the Agresso field trial. Carrying out an analysis require preparation was the analyst leader’s first analysis. It implied that the leader had to learn the CORAS methodology and the tool before perform the analysis. Accomplishing the analysis involves deciding when and how to perform it and compose a team to participate during the analysis meetings. Finally write an analysis report.

IL	Task Name	Start	Finish	2005				2006					
				Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun
1	Learning CORAS	12/09/2005	30/11/2005	█									
2	Planning the analysis	01/12/2005	09/01/2006				█						
3	Carried out the analysis	10/01/2006	21/04/2006					█	█	█	█		
4	Context identification 1	10/01/2006	10/01/2006										
5	Context identification 2	24/01/2006	24/01/2006										
6	Risk identification 1	01/02/2006	01/02/2006										
7	Risk identification 2	08/02/2006	08/02/2006										
8	Risk estimation and evaluation 1	14/03/2006	14/03/2006										
9	Risk estimation and evaluation 2	20/03/2006	20/03/2006										
10	Risk treatment	21/04/2006	21/04/2006										
11	Writing analysis report	21/04/2006	01/06/2006									█	

Figure 14 Milestones of the first investigation

Table 6 presents the analysis participants and their roles and responsibilities in the analysis.

Name	Role
Jenny B. Hougen	Analyst leader
Tor Gaute Indstøy	Security expert, system designer, analysis secretary
Erik Inge Marcussen	Developer, AGRESSO framework expert
Randi Bjørnbeth	System designer
Truls Tveøy	System designer, developer
Helge T. Blindheim	Customer view

Table 6 Roles and responsibilities among the analysis team

During the analysis process there several surveys were carried out. Table 7 gives an overview of how and when we collected the results from the team members.

Action type	Date	Participant	Description
Questionnaire 1	24.01.2006	Tor Gaute Indstøy, Erik Inge Marcussen, Randi Bjørnbeth, Truls Tveøy, Helge T. Blindheim	The questionnaire was performed after the first analysis meeting with all the participants. The results from this questionnaire are given in Appendix A.1.
Questionnaire 2	21.04.2006	Tor Gaute Indstøy, Erik Inge Marcussen, Randi Bjørnbeth, Truls Tveøy,	The questionnaire was performed after the last analysis meeting and the results are given in Appendix A.3
Interview	15.03.2006	Tor Gaute Indstøy, Truls Tveøy	There were carried out a interview on two of the participants. The questions from the interview are given in Appendix A.2
Observation	24.01.2006 – 20.03.2006	Jenny Beate Hougen	The analyst leader observed all the meetings with the team. The observations are presented as the analyst view in Chapter 6.

Table 7 How and when we collected evidence

4.3.3.2 Second investigation: CORAS according to IT-security standards

This field trial investigated organisations use of IT-security standards, and whether the standards used are those on which CORAS is based on. The investigation process is illustrated in Figure 15.

At first it was necessary to get an overview of IT-security standards available in the market. With basis in those available standards found a questionnaire were created. The questionnaire was sent to different organisations. The questionnaire is presented in Appendix B. The result from the survey are discussed and evaluated with respect to possible consequences for CORAS.

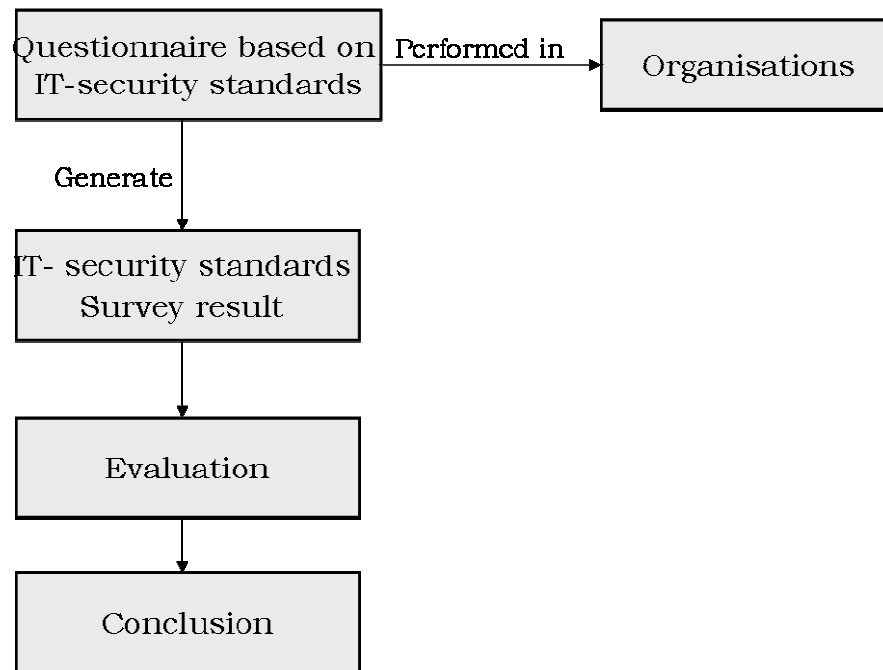


Figure 15 Overview of the second investigation

Figure 16 shows the milestones of the second investigation.

ID	Task Name	Start	Finish	2005		2006						Task Notes
				Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	
1	Prepare survey	01/11/2005	01/03/2006	██								Created and explored after known IT-security standards
2	Carry out the questionnaire	22/03/2006	07/04/2006					▼				
3	Abelia seminar Hand out questionnaire	22/03/2006	23/03/2006									Collected 12 results
4	Contact organisations	23/03/2006	07/04/2006					█				Collected 8 results

Figure 16 Milestones during the second investigation

4.3.4 Evaluation and discussion

The last process of the research was evaluating and discussing the results. Chapter 6 presents an evaluation of the results from the security analysis performed in Agresso. Chapter 7 presents an evaluation from investigating CORAS according to other IT-security standards. These evaluations are input to the discussion in Chapter 8.

Chapter 5

Hypotheses for the evaluation of CORAS

The starting point for the evaluation was a set of predefined hypotheses. The hypotheses were subsequently used together with the evidence collected during the research to discuss whether they were fulfilled or not. For the evaluation to be success the formulated hypotheses should be validated ideally either verified or falsified.

This chapter presents the hypotheses used to evaluate the investigation results. The next sections present the formulated hypotheses pursuant to the two investigations; the CORAS's framework and CORAS according to IT-security standards.

5.1 Hypotheses with respect to the CORAS framework

Since CORAS already has established requirements and goals, the hypotheses according to the CORAS framework are formulated with respect to these. Below is an overview of some of the requirements used as a basis [8]:

- *Security*: Help protect confidentiality, integrity and availability of data.
- *The CORAS methodology*:
 - Simple: It is easy to understand.
 - Efficient: More efficient than other similar tools.
 - Teamwork: Possible to cooperate and work well in teams.
 - Flexibility: Accommodate the user's needs.

- *The different user groups:* There are different requirements on how CORAS should work within the different groups. When doing security analysis the CORAS methodology requires involvement of different participants as risk analyst, developer, researchers, and decision makers.
- *The documentation:* Defines a way to document and store the results. The CORAS tool is meant for document and store the results. The tool should contain facilities to make complete standardised formats of the risk analysis report. They should be understandable and sensible, and accommodate the different user groups.

These requirements were considered when formulating both the hypothesis and the hypothesis sub-statement. In the next sections the hypotheses for the CORAS UML profile, the CORAS tool and the CORAS RMP is presented.

5.1.1 Hypotheses with respect to the use of the CORAS UML profile

CORAS UML profile is used to support the risk management process. To get a common understanding of the target of analysis, threats, vulnerabilities and risks is important in an analysis. The CORAS UML profile should support this [1].

In the security analysis process CORAS requires the involvement of different kinds of people. They are involved in different ways. It is common to distinguish between three main groups: the security analysis experts, system experts, and the users of the system. The security analysts are experts on CORAS, and are familiar with the elements and the strategy used in the analysis. The system experts are not familiar with CORAS, but they typically have a complete understanding of the system and the terms related to security. The users of the system normally have insignificant technical insight. They see the system from a non-technical view and have usually no security knowledge.

The challenge here is when the analysis team communicates. Due to the participants' different backgrounds and knowledge, misunderstandings may occur. Two people with different backgrounds will probably have different comprehensions of the same thing. E.g. a farmer and a building constructor may not have the same illusion of a high-class building (Figure 17). It is believed that the use of graphical drawings and models will solve such problems.



Figure 17 Communication problems

Together with the standardised modelling language UML and CORAS specific elements the CORAS developers believe that the communication between the analysis participants will be improved and avoid misunderstandings.

Can a model stand alone (Figure 18)? A model alone is not a good explanation, but a model together with a description is a good combination.



Figure 18 Can a model stand alone?

With these viewpoints as a basis, hypotheses were specified with respect to the use of the CORAS UML profile in the analysis process.

HYPOTHESIS 1: Terms and icons used in CORAS are intelligible for all parts involved in the analysis

- The security terms are well known
- The CORAS icons are intelligible
- UML is well known and serves an expressive way to explain the analysis objects

HYPOTHESIS 2: The unwanted incidents and treatment diagrams are easy to understand and support the analysis process.

- The diagrams are easy to understand
- Use of models improves the communication in the analysis team.
- Use of models prevents misunderstandings and mistakes among the analysis team.
- Use of models increases the efficiency of the risk analysis process.
- Use of models improves the process of finding possible threats and unwanted incidents

5.1.2 Hypotheses with respect to the CORAS tool

The purpose of the CORAS tool is to support to the methodology process. The tool should assist the CORAS experts to achieve efficient and good results. It should satisfy the requirement of good documentation. The tool offers ways to document and store results which allow the tool users to create their own experience library. The analysis expert could reuse previous analysis results and hence achieve efficient and good results. Based on the features created and saved during the analysis the tool can generate an analysis report. The tool also conducts a short tutorial of the steps in the CORAS methodology.

In order to reveal the quality of the CORAS tool the Hypothesis 3 was established.

HYPOTHESIS 3: The CORAS tool improves the analysis and increases the efficiency of the analysis

- The analyst leader finds it easy to learn the tool
- The tool gives a good description of the analysis steps
- The functionalities in the tool work as intended
- The report generator is good

5.1.3 Hypotheses with respect to the CORAS risk management process

It is not only important to understand the CORAS's terms, models and icons. The most important factor is to achieve a good result by delivering an analysis result

that is reasonable and useful. The overall objective is to find all relevant risks and to suggest a way of treating them.

An approach of CORAS is to please the customers. There are several factors involved when deciding whether an analysis was successful. Both the analysis team and the organisation's management should be satisfied. The CORAS customers should feel that CORAS gave them what promised. Some of the factors CORAS promises are cost-efficient analysis, good documentation and the possibilities for reuse. To determine if the analysis pleased the customer, there were specified hypotheses related to this.

HYPOTHESIS 4: The CORAS customer was pleased and intended to continue to use CORAS in the future

- The analysis process was efficient
- The risk analysis report was understandable and sensible.
- Use of security analysis will help the design team building secure and good systems.

During a CORAS RMP structured meetings are conducted. The results of these meetings are important according to the process of finding risks. There was of interest to find out whether the structured meetings are a good and efficient way of finding risks and whether the suggested composition of the team members is appropriate. This led to Hypothesis 5.

HYPOTHESIS 5: The result and the accomplishment of the analysis meetings was good

- The communication during the meetings was good
- The analysis meetings were efficient
- The composition of the team members with different backgrounds was appropriate

5.2 Hypotheses with respect to IT-security standards

According to the investigation of CORAS according to IT-security standards there exists no requirement. The goal of the investigation was to find out whether organisations use IT-security standards, and if the standards used are the same as CORAS is based on. The hypotheses are motivated from this goal.

The CORAS framework is based on several IT-security standards. CORAS is mainly based on Australian IT-security standard for risk management AS/NZS 4360. In Table 8 presents an overview of the standards on which the parts of the CORAS framework are based. [1] Of these standards there are only AS/NZS 4360,

ISO/IEC 17799, ISO 13335 and IEC 61508 are used for IT-security. As displayed in the table the AS/NZS 4360 is represented in all parts of the CORAS framework.

CORAS field	Standard
The CORAS terminology	AS/NZS 4360:1999, ISO/IEC 17799-1:1999, ISO/IEC WD 13335, IEC 61508, BS 4778:1991, ISO/IEC 10118
The CORAS methodology	AS/NZS 4360:1999
The CORAS Library	ISO/IEC 10746, AS/NZS 4360:1999

Table 8 Overview Standards CORAS is based on

By cover the use and need for such standards will probably also cover the need for CORAS. An appropriate question is the organisations' familiarity with, and adherence to, standards. The following hypotheses are related to this question (Hypothesis 6 and Hypothesis 7).

HYPOTHESIS 6: The CORAS framework is based on standards already in use among organisations

- The majority of organisations follow the AS/NZS 4360 standard
- The majority of organisations are familiar ISO 17799 standard
- The majority of organisations are familiar with ISO 13335
- The majority of organisations are familiar with IEC 61508

HYPOTHESIS 7: There is a need for good IT-security standards among organisations

- The use of IT-security standards makes the organisation more competitive
- IT-security standards are required by the organisations' clients
- Use of IT-security standards will increase the efficiency in the development process
- The use of standards improves the product quality and the development process quality
- The use of standards increases the customers trust in the products
- Organisations have much focus on standards both in the organisation and in the market

Chapter 6

CORAS field trial in Agresso

In order to investigate the validity of the hypotheses in Chapter 5.1 a major case study was accomplished; the security analysis in Agresso. In order to gather results there were performed surveys among the analysis participants. In addition the analyst leader collected experience during the analysis. This chapter evaluates the results collected during the security analysis in Agresso.

The structure of each chapter section is illustrated in Figure 19. Each section start with a presentation of the results gathered from the analysis team and the analyst leader's observations and experiences. Except for the CORAS tool section which only consists of the result from the analyst leader. The sections are arranged in the same order as the hypotheses in Chapter 5. The presented results are compared with the hypotheses from Chapter 5 for evaluation.

As presented in Chapter 4.3.3.1 there were performed two surveys and one interview referred as *Questionnaire 1*, *Questionnaire 2* and *Interview*. Each section refers to the particular questionnaire and interview where the results are obtained.

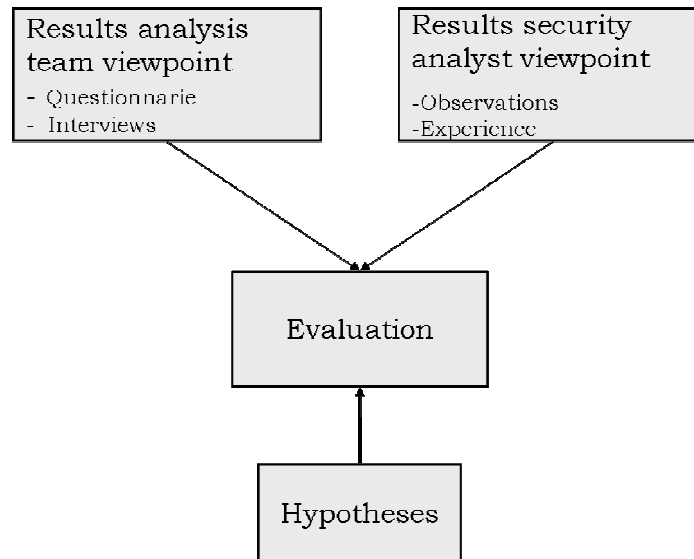


Figure 19 Chapter structure

The following subsections contain; an analysis summary, the results and evaluation of using the CORAS UML profile, the CORAS tool and the CORAS RMP.

6.1 Analysis summary

A security analysis was carried out in cooperation with Agresso in the period January to March 2006, targeting the AGRESSO system. The goal of the analysis was to identify risks related to the AGRESSO functionality and suggest treatments to identified risks.

The analysis a team consisted of six people with different backgrounds; a security expert, a system designer, a developer, a system expert, a customer representative and the security analyst. The team members had no particular experience with security analysis and only one team member had participated in a similar analysis.

The analysis team carried out seven meetings before the result was finished. An overview of the analysis meetings is given in Table 9. During the analysis there were collected results from questionnaires, interviews and observations.

Task description	Performed date	Participators	Description
Context identification	10.01.2006	Tor Gaute Indstøy, Erik Inge Marcussen, Jenny B. Hougen	Together with two of the team members the analyst leader established an understanding of the target. UML models of the target were created.

Task description	Performed date	Participators	Description
Context identification and approval	24.01.2006	Tor Gaute Indstøy, Erik Inge Marcussen, Randi Bjørnbeth, Truls Tveøy, Helge T. Blindheim, Jenny B Hougen	The team members were introduced to CORAS. The team achieved a common understanding of the target and identified assets.
Risk identification	01.02.2006	Tor Gaute Indstøy, Erik Inge Marcussen, Randi Bjørnbeth, Truls Tveøy, Helge T. Blindheim, Jenny B Hougen	Brainstorming. The group was separated into two subgroups. Each subgroup got UML diagrams from the context identification and an empty HazOp table for filling in the identified risks.
Risk identification	08.02.2006	Tor Gaute Indstøy, Erik Inge Marcussen, Randi Bjørnbeth, Truls Tveøy, Helge T. Blindheim, Jenny B Hougen	Continued the risk identification.
Risk estimation and evaluation	14.03.2006	Tor Gaute Indstøy, Erik Inge Marcussen, Randi Bjørnbeth, Truls Tveøy, Helge T. Blindheim, Jenny B Hougen	Frequency and consequence values were added to the identified risks.
Risk estimation and evaluation	20.03.2006	Tor Gaute Indstøy, Erik Inge Marcussen, Randi Bjørnbeth, Truls Tveøy, Helge T. Blindheim, Jenny B Hougen	Continued the estimation process. Evaluated each risk and decided what risks to treat.
Risk treatment	21.04.2006	Tor Gaute Indstøy, Erik Inge Marcussen, Randi Bjørnbeth, Truls Tveøy, Jenny B Hougen	Treatment approval and closing of the analysis.

Table 9 Overview analysis meetings

6.2 Using the CORAS UML profile

The intentions with the analysis was firstly to find out how well the analysis participants understand the CORAS UML profile, secondly to find out whether the use of models improved the analysis process.

This section presents analysis teams and analyst leader's viewpoint of the CORAS UML profile.

6.2.1 The analysis team's view

There is of relevance that the analysis participants received a short introduction of CORAS's elements and concepts before the Questionnaire 1 were handed out. The results are based on the knowledge they had after the introduction.

This section proposes the results from the team members' knowledge and opinions of the risk terms, the CORAS icons and the CORAS diagrams.

6.2.1.1 The risk terms

Risk terms are frequently used during an analysis process. The terms and icons used may be unknown for the analysis participants. Below is the result from the Agresso analysis participants knowledge of the terms and icons used in the analysis performed in Agresso.

Questionnaire 1 result

The participants were asked about their knowledge of certain risk terms. The results are displayed in Figure 20. In general most of the terms were familiar among the team. Three of the terms were familiar to the entire team. It was the "threat", "vulnerability" and "risk".

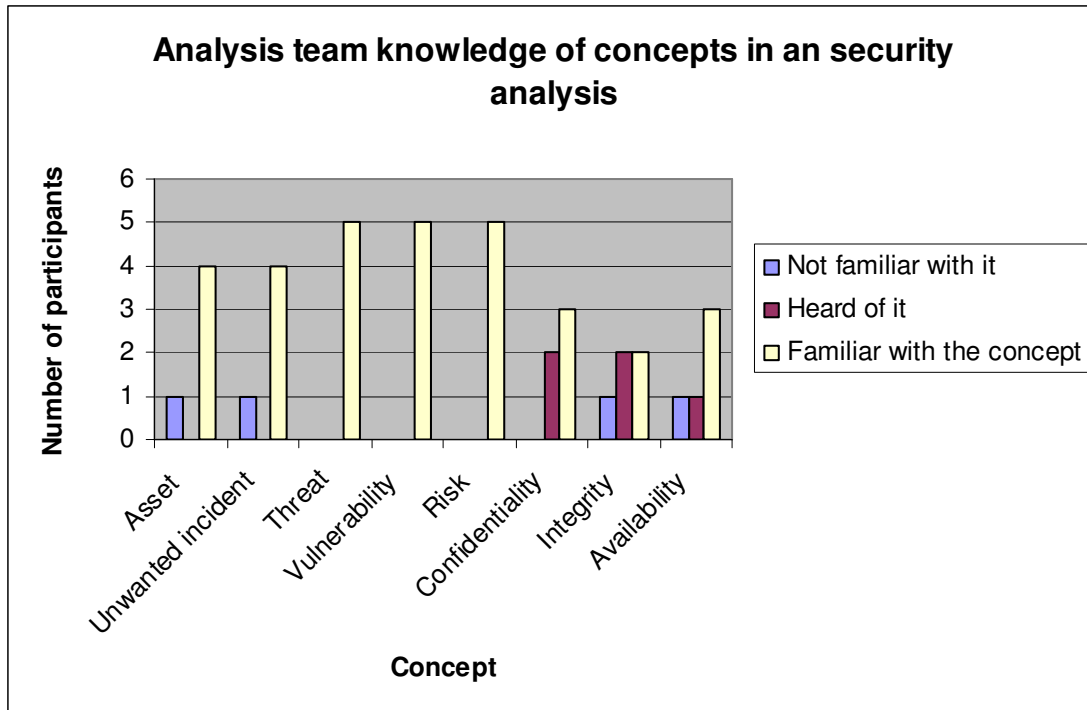


Figure 20 Knowledge of terms and concepts in a security analysis

Interview results

In the interview, the participants were asked if some terms had been more difficult to understand than others. The answers from the interviewees are given in Table 10.

Question	Interviewee	Answer
Were some terms more difficult to understand than others?	Team member 1	The term “asset” is not a much used word. It may be a bit unknown and the actual meaning of it is vague.
	Team member 2	Not a big problem to understand the concepts after they had been introduced.

Table 10 The interviewees’ knowledge of terms

6.2.1.2 The CORAS icons

The CORAS icons (elements) are used to create threats and unwanted incidents diagrams. The purpose is to create good visualised diagrams that are easy to understand for the analysis participants. The results from the analysis team’s opinion about the icons are presented below.

Questionnaire 1 result

After the first meeting the participants were asked whether they found the CORAS elements easy to understand. The results are displayed in Figure 21. It shows that the majority believed the CORAS element are easy to understand.

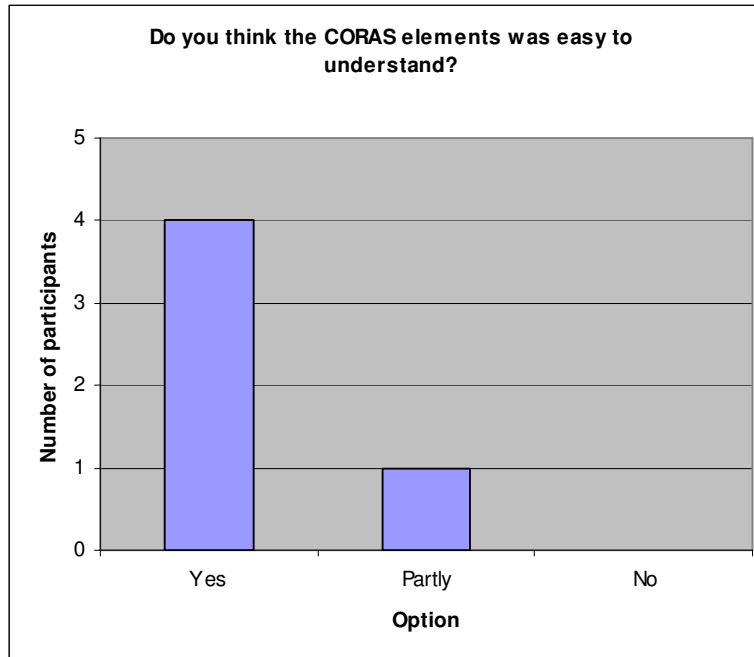


Figure 21 Participants understanding of the CORAS elements

Interview result

In the interview the participants were asked if the icons are difficult to understand. The result is presented in Table 11.

Question	Interviewee	Answer
Were the CORAS icons difficult to understand?	Team member 1	The icons were a bit difficult to understand. The comprehensibility depend that the participants have some general knowledge about analysis and the architecture around such an analysis.
	Team member 2	Not a big problem to understand the CORAS icons.

Table 11 Interviewees results comprehensibility of the CORAS icons

6.2.1.3 The CORAS diagrams

The CORAS diagrams are used to depict unwanted incident (threat) and their possible treatment. The diagrams are meant as a help to document and store the results and help the team members communicate and understand each other. This section represents the team judgement and understanding of the CORAS diagram.

Questionnaire 2 result

The CORAS diagrams inherit several aspects from UML. The participants UML knowledge may be relevant according to their understanding of the CORAS graphical language. In Questionnaire 2 the participants were asked whether they were familiar with UML. The result is given in Figure 22.

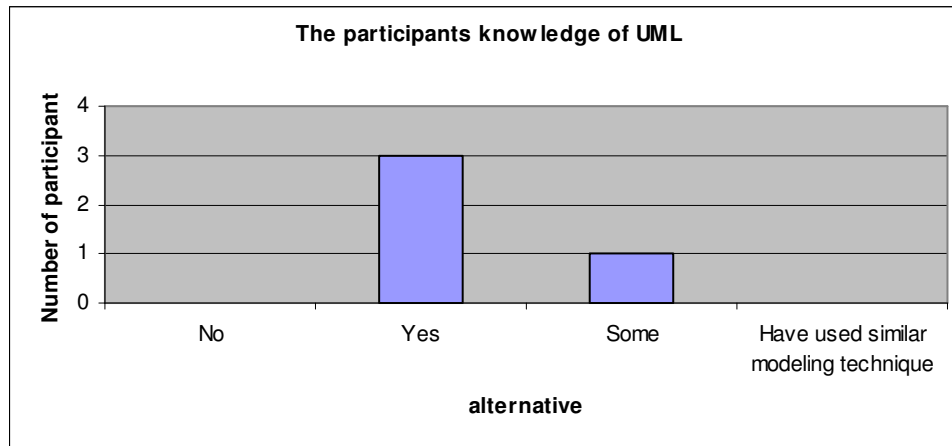


Figure 22 participants knowledge of UML

In order to find the participants opinion of the CORAS graphical language several propositions were stated. The participants' agreement rates are presented in Figure 23. Generally the participants believed that the use of diagrams had positive effect on the analysis.

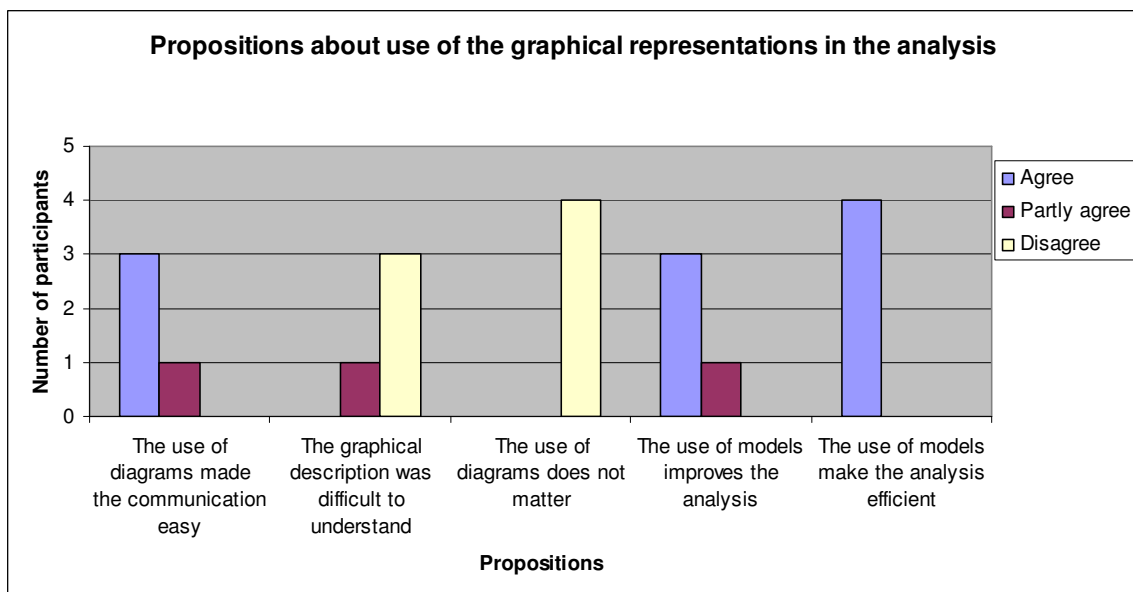


Figure 23 Participants opinion about the use of graphical languages

Interview result

The interviewees were asked what they thought of the CORAS diagrams, whether the diagrams were easy to understand and whether they represented a good way of displaying the results. The result is presented in Table 12.

Question	Interviewee	Answer
What do you think about the CORAS diagrams?	Team member 1	Difficult to understand. The analyst leader should have used more time explaining them. An idea is to let the team member try drawing it themselves.
	Team member 2	They were mainly self-explanatory. Easy to understand since I have been modelling a lot. Joining the diagrams with the HazOp table was a good combination. Use of diagrams to visualise is good. The CORAS diagrams were good to visualise the risks.

Table 12 Interviewee results of the CORAS diagrams

6.2.2 The security analyst's observations

This section gives the result from the analyst opinion of the CORAS UML profile. The results are based on the analyst's own experience of the analysis and the analyst's observation of the analysis team. Table 13 gives the analyst result on the CORAS UML profile.

Viewpoint	Result
The risk terms	<p>The analyst leader was not familiar with the term "asset" before learning the CORAS method. It is a term that is not frequently used in other contexts.</p> <p>The analyst gained knowledge about the team after seeing them in action. Based on that the analyst leader believe that some of the terms like asset and unwanted incident would not have been insufficiently understood if not explained.</p>
The CORAS icons	<p>The threat scenario icon and threat agents used in the diagrams were related to terrorist and terror by the team members.</p> <p>By using the Figure 9 (in Chapter 2) when introducing CORAS it helped the team to understand the terms better.</p>
The CORAS diagrams	<p>It seemed difficult for the team members to distinguish between unwanted incidents and threat scenario, but the diagrams made it easier for the team to indicate agreement, disagreement and change. Thus it made the communication easier and probably more efficient. A common interpretation of the diagrams would probably improve the analysis process.</p> <p>The use of models made it easier to start conversations and express opinions among the team. This probably resulted in less misunderstandings and mistakes.</p>

Table 13 Security analyst viewpoint of the CORAS UML profile

6.2.3 Evaluation of the CORAS UML profile

Bellow follows an evaluation of Hypothesis 1 and Hypothesis 2 in Chapter 5.1.1 based on the previous result. It is important to have in mind that the questionnaire results may have taken another direction if the survey were performed before the participants were introduced to CORAS.

HYPOTHESIS 1: Terms and icons used in CORAS are intelligible for all parts involved in the analysis

- The security terms are well known
- The CORAS icons are intelligible
- UML is well known and serves an expressive way to explain the analysis objects

The security terms are well known. The use of risk terms is frequent used in a security analysis. The concepts may be difficult to understand for people unfamiliar with security analyses. According to the Agresso analysis team there was different knowledge of some of the terms used.

“Threat”, “vulnerability” and “risk” were terms the team had no problem to understand. It could be because those are words we use in the daily life.

Four of five were familiar with “unwanted incident” and “asset”. The fact that one was not familiar with the words may be because of the analyst leader’s presentation was vague and that the team members had difficulties understanding the meaning of it. It may be difficult to understand some of the words because they are not frequently used and the meaning of it may be confusing (as pointed out by the interviewees in Table 10).

The terms “confidentiality”, “integrity” and “availability” are security related words. The knowledge of these words is different among the team members. It could be related to that the knowledge of IT-security distinct between the team members. One out of five was not familiar with “integrity” and “availability”. “Integrity” seems to be more diffuse than “availability”. None of the team members had problems understanding “confidentiality”. The reason could be because the term “confidentiality” is used in other relations than security.

It seems that the understanding of risk terms is related to the analysis participants’ background and the analysts’ explanation. It also affects the teams understanding, whether the word is self explanatory or used frequently in other relations.

The CORAS icons are intelligible. The purpose of the CORAS icons is to express graphically such that everyone involved in a CORAS risk analysis can understand.

The survey result in section 6.2.1.2 indicates that the analysis participants found the CORAS elements (icons) easy to understand. But when interviewed, Team member 1 thought the icons was a bit difficult to understand (Table 11). The survey was performed after the context identification meeting and before the icons was

used in any diagram. The interview was performed after the risk identification meetings where the icons were used in diagrams.

By observing, the analyst noticed that the threat scenario and threat agent icons were associated to terror and terrorist by the team members (Table 13). To some people this appears improper.

UML is well known and serves an expressive way to explain the analysis objects. The participants' knowledge of UML may be indicative of the participants understand and favour the CORAS models. According to the result in Figure 22 all the participants were familiar with UML, thus this results indicates that UML is well known.

As presented in Figure 23 the participants disagreed that the use of diagrams in an analysis is irrelevant. One of the participants partly agreed that the diagrams were difficult to understand when the others disagreed. Thus pursuant to this analysis, the participants found the way of explaining the analysis objects to be understandable and not wasted, but it can not be concluded that this is the best way to do it.

Conclusion. It is important that the analysis participants have the same understanding of the words and concepts used in an analysis. The participants' backgrounds may be essential for in their knowledge of risk terms and understanding of the icons. In this analysis the risk terms and CORAS' icons were not essential problem for the participants. UML was a known technique among the team, but do the team thinks it is an expressive way to explain the analysis objects? To answer the HYPOTHESIS 1 the statement is true according to this analysis if the team gets a short introduction to CORAS. Since the team were familiar with UML this may also be a reason that they found it easy to understand the icons.

HYPOTHESIS 2: The unwanted incidents and treatment diagrams are easy to understand and support the analysis process.

- The diagrams are easy to understand
- Use of models improves the communication in the analysis team
- Use of models prevents misunderstandings and mistakes among the analysis team
- Use of models increases the efficiency of the risk analysis process
- Use of models improves the process of finding possible threats and unwanted incidents

The diagrams are easy to understand. The CORAS diagram should be easy to understand for everyone involved in the analysis. In the interview of the two team members (Table 12) they had different opinions on the comprehensibility of the diagrams. Team member 1 found the diagrams difficult to understand. He believed that the analyst leader could have explained the diagrams more and that the team could be involved in the process of drawing the diagrams, then they would be easier to understand. Team member 2 had a different opinion; he found the

diagrams to be mostly self-explanatory. The combination of the threat diagram together with a description of the diagram in the HazOp table was good, he thought.

The reason for the various answers from the two team members may be of their different background knowledge. Team member 2 has much experience in modelling. If Team member 1 does not have experience with modelling that may be a reason that he found it difficult to understand the diagrams.

Use of models improves the communication in the analysis team. Visualising threats and unwanted incidents will probably improve the communication among the team participants. By using models makes it easier to indicate where to make changes and where to agree or disagree. As presented in Figure 23 three (75 %) of the team members agreed to the hypothesis that use of diagrams made the communication easy while one partly agreed. The analyst's impression was that models made the process easier.

Use of models prevents misunderstandings and mistakes among the analysis team. Different people with different backgrounds are involved in a security analysis. This fact often results in different comprehensions and misunderstandings among the team. The purpose of using models is to avoid the misunderstandings.

According to the analyst's experience in Table 13 the use of models led to fewer misunderstandings among the team. The result in Figure 23 shows that three of the team members believed the use of models improved the analysis while one partly agreed.

Use of models increases the efficiency of the risk analysis process. Underlying this statement is the anticipation that models-based in a security analysis will improve the communication flow and reduce misunderstandings. Thereby, the analysis process will probably be more efficient. All team participants agreed that the use of models made the analysis more efficient.

Use of models improves the process of finding possible threats and unwanted incidents. It is difficult to decide if the use of models improved the risk identification process. There is no specific result which indicates that the use of models will improve the process. But good communication, less misunderstandings and efficiency are elements that will have impact on the result. If the models improve these elements they will probably improve the process of finding threats and unwanted incidents.

Conclusion. The use of models such as the unwanted incident and threat diagrams are meant to support the analysis process. To support the analysis process the models must be; simple to understand, help improve the communication, help avoid misunderstandings, and increase the efficiency of the analysis. In addition the models may help finding possible threats. In general, the participants of this analysis found that the models were eased comprehension and improved communication. It was not possible to tell from the results if the use of models increased the analysis efficiency, reduced misunderstandings or improved the

process of finding threats. Thus in order to answer Hypothesis 2 there was lack of results and it is not able to answer. The hypothesis is not verified, but remains provisional.

6.3 Experience with the CORAS tool

The CORAS tool was used by the analyst leader during the analysis process. This section presents the analyst experience of the tool. The purpose was to find out whether the CORAS tool satisfies its intention or not. The results are compared with the Hypothesis 3 in Chapter 5.1.2.

6.3.1 Results from using the CORAS tool

The CORAS tool offers different functionalities. Whit regard to this analysis the tool was used for three purposes:

- *As a guide through the analysis:* The tool was used as a guide when performing the analysis.
- *Create and save the analysis project results:* The analyst used the tool to create a project for the analysis performed. During the analysis process the findings were saved in the particular project.
- *Generate an analysis report:* When the analysis was finished the tool generated a report on the results and saved in the analysis project.

Through these three user areas the analyst gathered experience through learning and using. The next sections present the analyst's observations from learning the tool, using the CORAS methodology guide and by using the different functionalities in the tool (e.g. creating tables, importing files, using the diagram editor or generating the analysis report)

6.3.1.1 The process of learning the tool

The analyst had no experience from other risk analysis tools and was first introduced to the CORAS tool version 2.0 in August 2005. This version had some problems and a new version 2.0.1 was released in October 2005. This result is based on the new release of the tool.

The process of learning the tool was by trying it on a small case before using it in a real organisation. These results are gathered from both cases. Disadvantages and advantages with learning the tool from the analyst viewpoint are illustrated in Table 14.

Status	Description
<i>Disadvantages</i>	To start the tool, we must first start the server and then start the client.
<i>Advantages</i>	Easy to understand for users that are familiar with similar tools.
	Easy to navigate
	Logical tool structure

Table 14 Results from learning The CORAS tool

6.3.1.2 Using the CORAS methodology guide

A feature of the tool is the CORAS methodology guide that describes the analysis process. The guide suggests accomplishing activities and sub-activities during each step of the analysis. The analyst followed this guide through the analysis process and identified advantages and disadvantages based on the experience through the analysis process (Table 15).

Status	Description
<i>Disadvantages</i>	If the analysis expert is not familiar with CORAS some CORAS-related expressions and words may be insufficiently explained. Explanations should include examples of the different actives.
	Missing a “Home” option that brings you back to the first page of the methodology guide.
<i>Advantages</i>	The guide is well structured and offers good help when it comes to remember the different activities

Table 15 Results from using the CORAS methodology guide

6.3.1.3 Using the functionalities in the tool

The tool offers different functionalities to support the activities in the methodology and store the analysis result. The user can create the methodology’s suggested tables and diagrams. Table 16 presents the results from using these functionalities during the analysis. The table is divided into different functionalities that exist in the tool. The functionalities may list deficiencies, errors and advantages.

Functionality	Status	Description
<i>Diagram editor</i>	Deficiencies	No ability to add user-defined icons.
		The vulnerability icon is missing.
		The elements in the editor are not up to date. .
	Advantages	An undo function exists.
<i>Table</i>	Deficiencies	No opportunity to create additional columns in a table.
		Missing a restore opportunity when deleting a table column.

Functionality	Status	Description
		No opportunity to create user-defined tables.
		Changing the column size or row size is not allowed.
		It Should be possible to remove rows in the Value of definition table.
		Not Possible to mark out rows or columns. It is only possible to mark out one field at a time.
		The Target of Evaluation (ToE) table should change name to Target of Analysis (ToA). ToE was the old name of this table.
	Error in the functionality	The objectives row in the Target of Analysis table is missing.
		The risk matrix table should name the low/medium/high columns consequence (see Figure 24). This could be done by e.g. adding a row above the low, medium and high cells.
		The predefined tables are linked to the appropriate folder in the risk analysis project.
	Advantages	Detail fields can not be removed. We have to manually remove the fields when the report is generated.
	<i>Report generator</i>	Deficiencies
With the 8 pt font size of the generated report makes it hard to read.		
It is not possible to generate a report when the name of the elements (tables etc.) stored in the project is three characters or less.		
There is no list of tables.		
There is no list of figures.		
It is not possible to update the table of content because the formatting is not used correctly.		
Error in the functionality		The detail viewpoint fail to appear in the generated report
		No save option. It should be possible to save an element before closing. The user has to close tables, diagrams etc. to save work.
		The document print-out displays erroneous page number. E.g. Page 9 of 43 becomes Page 9 of 9.
<i>General</i>		Deficiencies
	Impossible to delete several files/elements at the same time.	
	Impossible to alter the location of the	

Functionality	Status	Description
		imported element. E.g., an element in the risk identification folder cannot be moved to the risk analysis folder.
	Error in the functionality	The Risk analysis folder in the project view should be named Risk estimation as in the methodology guide.

Table 16 Results from using the tools functionalities

Frequency	Low	medium	high
usual	Low	Low	Low
rare	Low	Medium	Medium
Very rare	High	High	High

Figure 24 Table errors in the Risk matrix

6.3.2 Evaluation of the CORAS tool

The results were evaluated based on Hypothesis 3 from chapter 5.1.2. Below is a discussion whether the Hypothesis is fulfilled or not.

HYPOTHESIS 3: *The CORAS tool improves the analysis and increases the efficiency of the analysis*

- The analyst leader finds it easy to learn the tool
- The tool gives a good description of the analysis steps
- The functionalities in the tool work as intended
- The report generator is good

The analyst leader finds it easy to learn the tool. Before testing the tool on people with different knowledge of similar tools, it can not be proved whether it was easy to learn the tool or not. But according to the analyst experience the tool was easy to learn.

One drawback was that the CORAS-server has to run before the CORAS-client can start. The user should not have to start more than one service when starting a program.

After the analyst had started the tool, there was no big difficulty learning the tool and the analyst find it structured and easy to navigate.

The tool gives a good description of the analysis steps. During the analysis process the CORAS methodology guide were used by the analyst to follow the recommended activities in the process. The analyst found it difficult to understand some of the activities. The reason could be that the analyst was not familiar with CORAS. The analyst requested examples on the different activities. There should be a “home” option that returns to the first page.

The analyst finds it structured and well described. The description of the steps in the analysis is good if you are familiar with CORAS, but there should be more examples of the different activities.

To summarise, the methodology description is structured and easy to follow, but there is a lack of examples.

The functionalities in the tool work as intended. Most of the functionality in the tool was logical. It was easy to navigate. But it requires that we are familiar with similar tools and have knowledge about computer science. There were deficiencies and errors in the program functionality. These are displayed in Table 16. Some of these errors decreased the analysis process performance.

There were not found any particular errors with the diagram editor. But there exist some deficiencies. It is only possible to use the icons that already exist in the tool. The opportunity to add user-defined icons is missing. Because of this deficiency the drawings were created in another editor.

As in the diagram editor there exists deficiencies in the table functionality. The tool allows the user to create tables based on the activities in the analysis. The advantage is that it helps to add the tables in the correct part of the analysis. Some tables are predefined with row and column size. A lack is that it is not possible to change the column size and there is only possible to mark out one field in a table. This means that if we want to copy the entire table we can only copy one field at a time. This will slow down the process. The fact that it is not possible to change the column size in the editor that means we have to wait until the report is created and change it in the document which easily could be avoided. If these flaws were avoided, the performance would increase. Another error is the missing consequence name in the risk matrix.

A general deficiency in all the functionalities is the undo opportunity. There exists no undo function which means that if we accidentally delete a table it would be lost. It results in more time used, because the table has to be created over again. Another feature that was missed during the time using the tool was the opportunity to save elements when working with them. When creating large tables or advanced models it is required to save work during the process, because it is not desired to lose the work if the program accidentally shuts down. This is not an opportunity in the menu.

To summarise there is quite a lot which remains to be done before the functionality of the tool is good enough. Among the major flaws are lacks of undo and save opportunity.

The report generator is good. There exists a major error in the report generator functionality. It is not possible to generate reports when the analysis elements'

name is three characters or less. It is almost impossible for a user to guess what makes the error, hence for a user that gets this error it would be difficult to generate a report or the user would use a lot of time to figure out what makes the error. Another thing missing in the report generator was to be able to decide what to include in the report. Not all of the detail fields are necessary in every analysis. In addition the viewpoint field in the detail section is not a part of the detail section of the generated report.

The pictures in the generated report are too big for the document and you can only see half of them. Hence there will take time to change the size of each picture. To summarise, the report generator is not flexible (cannot choose what elements to include, font size and type etc.). It has this major error which can result in frustration and wasted time for the user. Thus it does not do the work efficiently many fixes remain before the report generated can be evaluated as good.

Conclusion. To answer the Hypothesis 3, there are still many features of the CORAS tool which should be improved. The tool is easy to learn and the methodology description is OK, there are a lot of deficiencies and errors in the functionalities and the report generator was not good. Thus the tool does not make the analysis process more efficiency. It is a help in the way that all the analysis results are structured and gathered in one place. The present condition of the tool does not offer help in the analysis process, but when the disadvantages are removed the tool will be helpful.

6.4 The CORAS risk management process

This section gives the results of the CORAS RMP. While carrying out the CORAS RMP it involves using the CORAS UML profile and the CORAS tool. The section gives the analysis team's view and the analyst view of the entire process. These results are estimated with the Hypothesis 5 and Hypothesis 6 from 5.1.3.

6.4.1 The analysis team's view

The CORAS UML profile and the CORAS tool are both a part of the CORAS RMP. They are elements to support the analysis process. This section covers the team's view of the CORAS RMP and the things that may influence the process.

6.4.1.1 The analysis team

The analysis team were asked whether they think a security analysis is useful. Two of the team members were of the opinion that a security analysis always is useful and the remaining three found a security analysis useful in some cases.

Interview result

The interviewees were asked about their opinions of the team composition. The results are displayed in Table 17.

Question	Interviewee	Answer
What do you think of the team composition?	Team member 1	There were too many participants with a system development view. There should been more with a customer view. The number of participants was appropriate.
The number of team participants?	Team member 2	The number of participants was appropriate. More people would affect the conversation; it would be more unnecessary chatting. Less people would be too few.

Table 17 Interviewee opinion of the analysis team

Questionnaire 2 result

Proposition of the analysis team were stated and the participants were asked whether they agreed or not. The results are given in Figure 25.

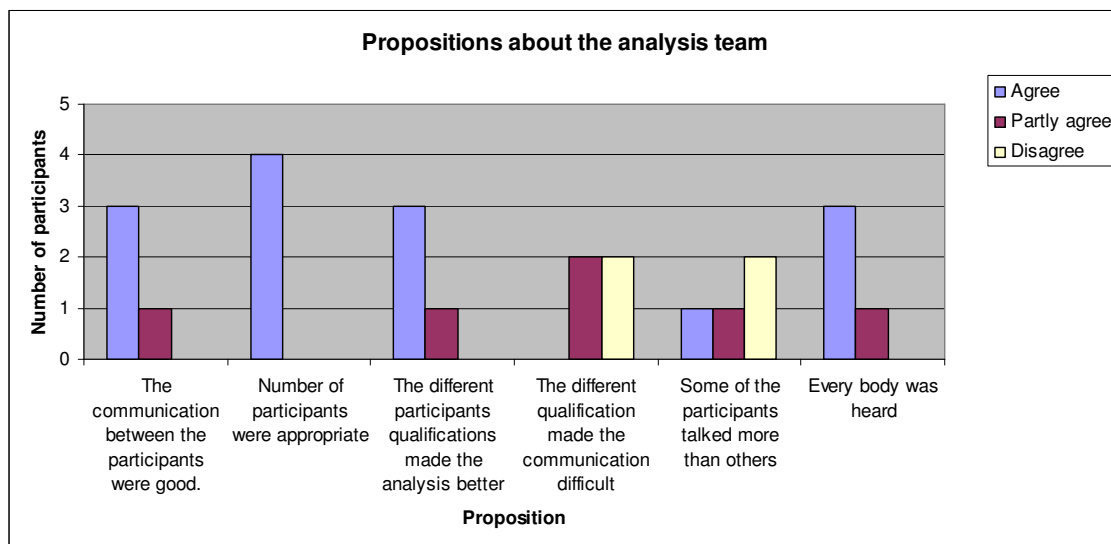


Figure 25 The analysis team opinion about the team

Table 18 presents the answers and comments where the participants were asked about the number of participants appropriate in an analysis.

Question	Option	Answers
The number of participants most appropriate in an analysis?	Less than 5	0 (1)
	5-6	3 (4)
	7-9	0
	Various	0
	Comment	One of the questionnaire participants meant it should be less than five or 5-6 participants. Therefore the numbers in parenthesis. There

Question	Option	Answers
		were totally four participants in this questionnaire.

Table 18 Questionnaire 2 result on number of participants in an analysis

6.4.1.2 The analysis meetings

The CORAS risk management process suggests accomplishing several meetings with the organisation in order to perform an analysis.

Interview result

In the interview the team members were asked what they think of the communication on the meetings (presented in Table 19).

Question	Interviewee	Answer
What do you think of the communication during the meetings?	Team member 1	The communication was OK. There was not much diversion.
	Team member 2	The communication was pretty much good. But it was sometimes difficult to understand what the other participants meant, specially the participants that had another background in the project.

Table 19 Interviewee opinion of the communication during the meetings

The interviewees were asked what they thought about the risk identification meeting, whether it was effective and whether it would be good to involve other people during the process. The result is presented in Table 20.

Question	Interviewee	Answer
What about the risk identification meeting? Was it effective?	Team member 1	Of course there are things that could be improved, but altogether it was efficiency. Splitting into groups (Buzzgroups) was not necessary. In this case it was not ideal to involve other people or change the team during the process.
Should it involve other people?	Team member 2	The brainstorming session could be done differently.

Table 20 Interviewee opinion of the Risk identification meeting

Questionnaire 1 result

To get an impression of the analysis participants' opinion of the Context identification meeting they were asked to give their agreement of the propositions. The result is given in Figure 26.

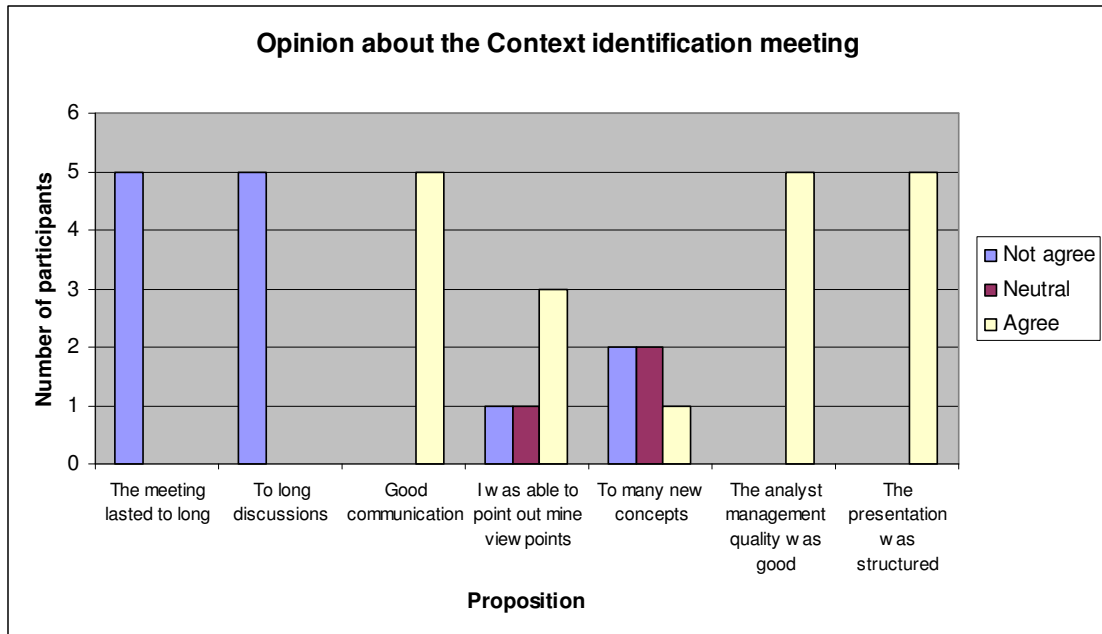


Figure 26 Analysis team opinions on the Context identification meeting

6.4.1.3 The analysis process in general

The participants were asked about their expectations, the analysis efficiency and future use of analysis in Agresso. All the results presented are achieved from Questionnaire 2.

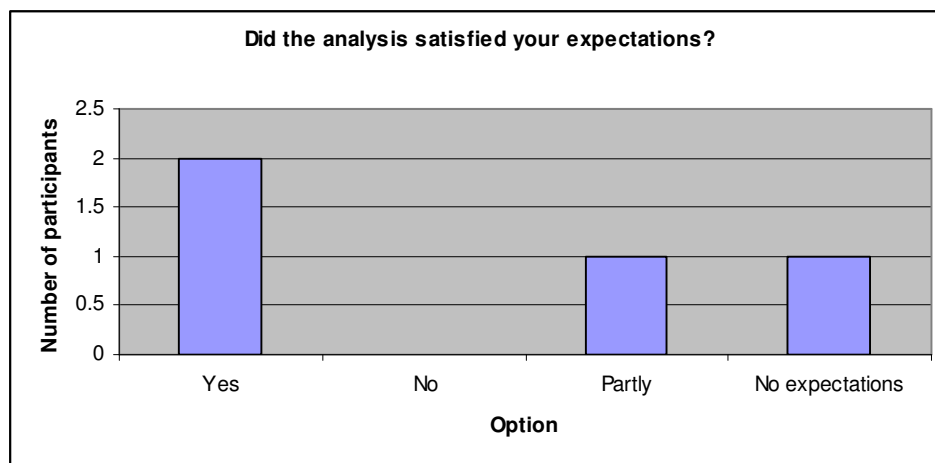


Figure 27 Results of whether the analysis satisfied the teams' expectations

In addition to the questions the participants in the questionnaire may add comments. The comments to the question from Figure 27 are presented in Table 21.

Comment	Comments on the analysis expectations:
Comment 1	My expectations were to learn about methodology and I got the chance.
Comment 2	I did not have much expectations since I never have participated on a security analysis before

Table 21 Comments to Figure 27

Table 22 gives the results from the participants' answer of what part of the development phase to perform a security analysis. The alternatives given to the participants were: All, before design, before implementation, after most of the implementation are finished, when the system is finished.

Question	Participant	Answer
In what part of the design phase is it most appropriate to complete a security analysis?	Team member 1	Before design. Adding it to the design phase to have more definite to discuss could be advantageous
	Team member 2	Before design
	Team member 3	Before design and after most of the implementation is finished
	Team member 4	During the design process

Table 22 Questionnaire 2 opinion about what part of development phase to perform an analysis

Figure 28 establishes a comprehension whether the team believed the analysis process were effective or not.

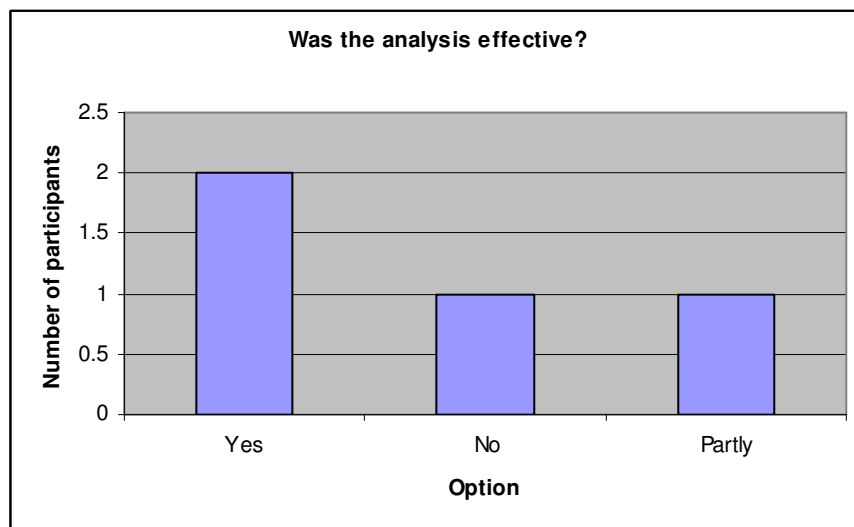


Figure 28 The analysis participants' opinion of the analysis efficiency

In addition to the questions in Figure 28 the questionnaire participants could add comments. The comments to the question are presented in Table 23 Comments to Figure 28.

Comment	Comments on the analysis efficiency:
Comment 1	A bit difficult to focus on one particular point.
Comment 2	(No) The analysis performed was too heavy to be used by all teams in Agresso. It was relatively time consuming, thus to use it as a part of development process for all teams would be difficult.

Table 23 Comments to Figure 28

Figure 29 displays whether the analysis team believed Agresso should have similar analyses in the future.

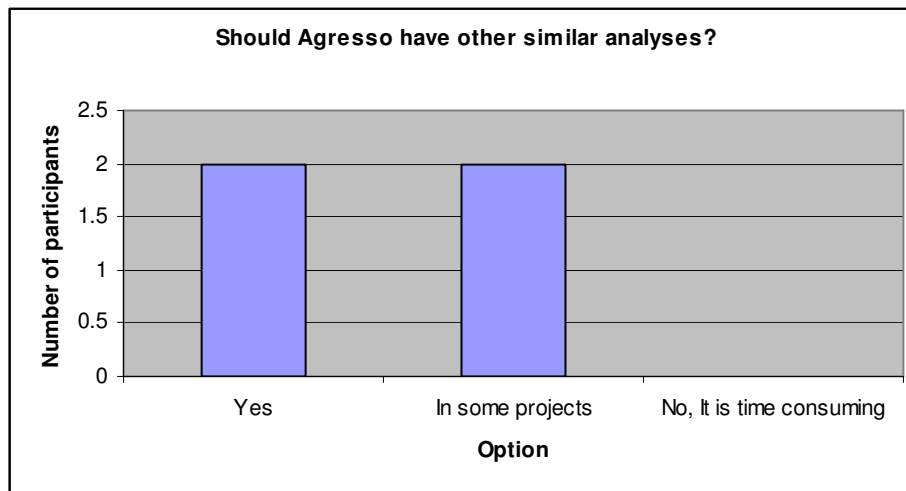


Figure 29 Future use of analysis

6.4.2 Security analyst observations

The analyst leader observed the team and the accomplishment of the meetings during the analysis process. The analyst's opinion about the team and the analysis meetings is presented in Table 24 and Table 25.

The team	Analyst opinion
The communication	There were no problems to communicate during the meetings.
Team roles and composition	The composition of the different team roles was very good. Maybe it should be one more with customer view.
Number of participants	There should be no more than six participants. Because to simultaneous find available time for all participants were difficult.

Table 24 Analyst observations about the analysis team

Analysis process	Analyst opinion
Context identifications	The context identification meeting went well. No specific problems. The communication was good. But the CORAS elements should probably have been better explained.
Risk identification	It was difficult to get the communication started and to direct the team in right direction. Each of the two meeting lasted 2-3 hours. These meetings should not last for more than two hours without a break. It was not necessary to divide the groups into two.
Risk estimation and evaluation	The challenge here was that there were no results from earlier analyses. There existed no logs or information that could help estimate the consequence and frequency values.

Table 25 The analyst observations about the analysis meetings

The analyst general impression of the entire analysis is given in Table 26.

Question	Analyst opinion
In what part of the development process is a security analysis most useful?	A security analysis should be accomplished together with the design phase or before the design.
Was the analysis effective?	The meetings were effective. The report generator decreased the analysis performance because of the deficiency and error in the functionality.
The CORAS graphical language	The diagrams are easy to understand when accompanied by description and if the participants are familiar with the terms used in the security analysis.

Table 26 The analysis process in general

6.4.3 Evaluation of the CORAS risk management process

This section evaluates Hypothesis 4 and Hypothesis 5 based on the results from Section 6.4.1 and Section 6.4.2.

HYPOTHESIS 4: The CORAS customer was pleased and intended to continue to use CORAS in the future

- The analysis process was efficient
- The risk analysis report was understandable and sensible
- Use of security analysis will help the design team building secure and good systems

The analysis process was efficient. One purpose with the CORAS RMP is that it should be effective and time consuming. It is one of the factors that would probably contribute to organisations future use of CORAS. It is difficult to measure the effectiveness of an analysis. The analysis could e.g. be compared other similar analyses. The result in Figure 28 indicates the average team opinion of the analysis efficiency. According to one of the participant the analysis was too heavy to be accomplished on all the functionalities in Agresso.

The risk analyst report was understandable and sensible. This statement could not be answered since there do not exist any result pursuant to it.

Use of security analysis will help the design team building secure and good systems. There exists no result to evaluate this statement.

Conclusion. It is difficult to verify the Hypothesis 4 since the results are insufficient. All the statements were diffuse.

HYPOTHESIS 5: The result and the accomplishment of the analysis meetings was good

- The communication during the meetings was good
- The analysis meetings were efficient
- The composition of the team members with different backgrounds was appropriate

The communication during the meetings was good. There was generally agreement that the communication between the analysis participants were good. According to Figure 25 there was different opinion if some participants talked more than others. The reason for this may be that the persons that talked more than the others did not feel they talked more. The agreement of the proposition “everybody was heard” implies that even if some talked more than others there was not necessary negative. In the proposition “The different qualifications made the communication difficult”,

half of the team agreed. Altogether the team seemed satisfied with the communication.

The analysis meetings were efficient. According to Figure 28 there was only one participant that did not believe the analysis meetings were efficient. In order to verify whether the analysis meeting were effective we need more information about why it was efficient.

The composition of the team members with different backgrounds was appropriate. According to both the interview results, the questionnaire result and the analyst opinion the number of participants in the analysis were appropriate. The only objection was that there were too many with development background. It should rather be one more that represent the organisations customer. Figure 25 shows that there were agreement of that the different qualifications among the team improved the analysis.

Conclusion. Two of statements in the Hypothesis 5 were verified. In order to answer whether the analysis meetings were effective, there should have been gathered additional information about why the meetings were effective. Thus the Hypothesis could not be fully verified.

Chapter 7

CORAS according to IT-security standards

The CORAS framework is based on several standards for security and risk management. [1]. This investigation purpose was to find out whether organisations need CORAS and whether the standards used are the same as those on which CORAS is based. To answer these questions a survey among twenty different organisations was accomplished. The result of the survey was used to answer the hypotheses in section 5.2.

This chapter will give the results from the survey and an evaluation of the result. Before the results and evaluation are presented a summary of the survey process is given.

7.1 Summary of IT-security standard investigation

A questionnaire was designed for the purpose of covering the organisations' use of IT-security standards. The questionnaire should be short enough so the organisations would take the time to answer it. The questionnaire created is given in Appendix B.

The challenge was how to make the organisations answer the questionnaire. The goal was to get at least twenty answers from different organisations. On an Abelia (www.abelia.no) seminar the 23 of March there were 43 organisations represented. The participants were asked to complete the questionnaire. Twelve results were collected. The following weeks different organisations were contacted to get at least eight more results. On the 8 of April the goal of twenty collected results were accomplished.

7.2 Results from IT-security standard investigation

The survey results are divided into three parts; information about the organisations, organisations' opinions on the use of IT-security standards, organisations' use of IT-security standards.

7.2.1 About the organisations

General information about each organisation was collected. The questionnaire started with questions about the organisation's size, type of organisation, type of customers and the degree of software development. This section presents the result of these questions.

The result in Figure 30 shows that most of the organisations that participated in the investigation have more than or equal to three hundred employees.

Less than 25: 20%

26 – 100: 25%

101 – 300: 5%

More than 300: 50%

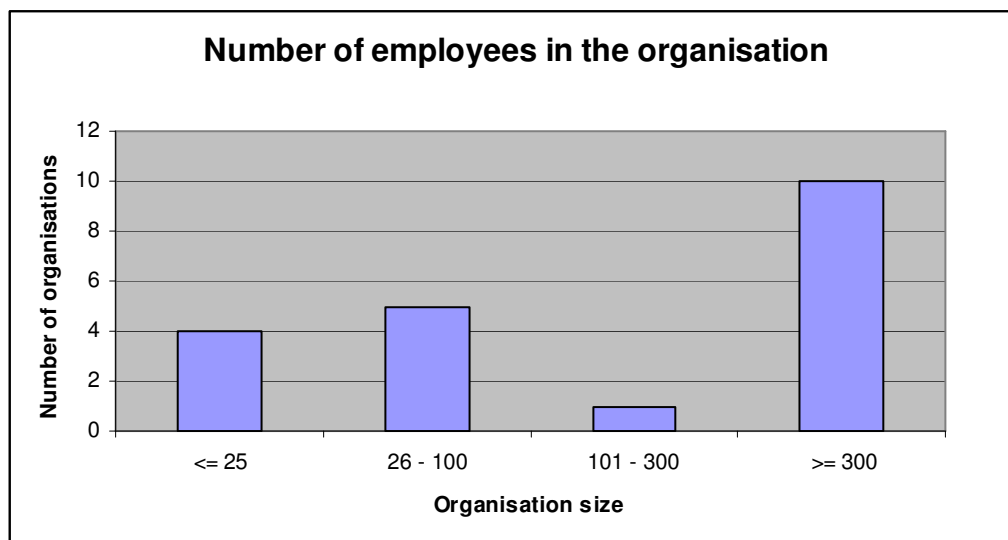


Figure 30 Overview organisation size

The result in Figure 31 illustrates the selections distribution between public and private sector. It indicates that the organisations participated were mostly private.

Private: 85 %

Public: 10 %

Other: 5%

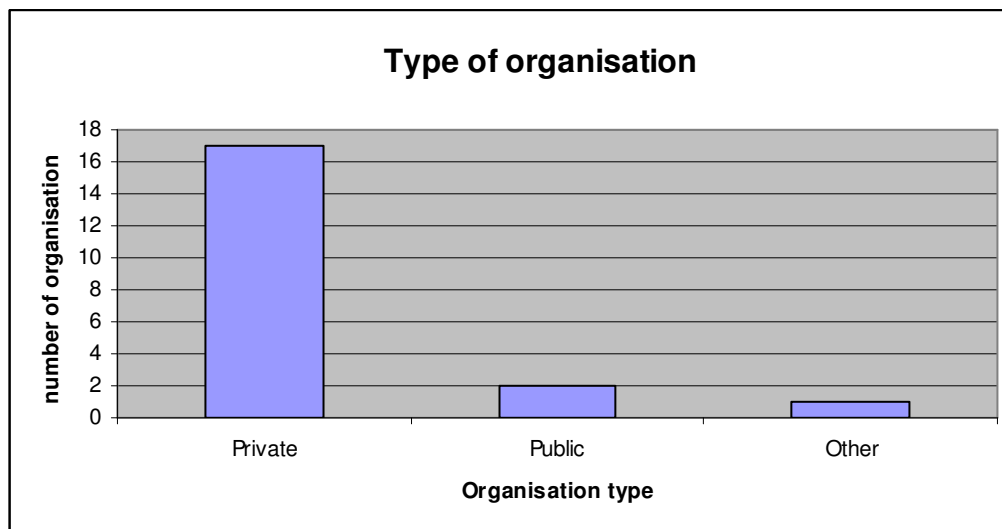


Figure 31 Overview organisations types

Figure 32 presents the organisations' type of customer. As illustrated in the figure the organisations' customers are generally from the private sector or from both sectors.

Customers in public sector: 10 %

Customers in private sector: 40%

Customers equally in both sectors: 50%

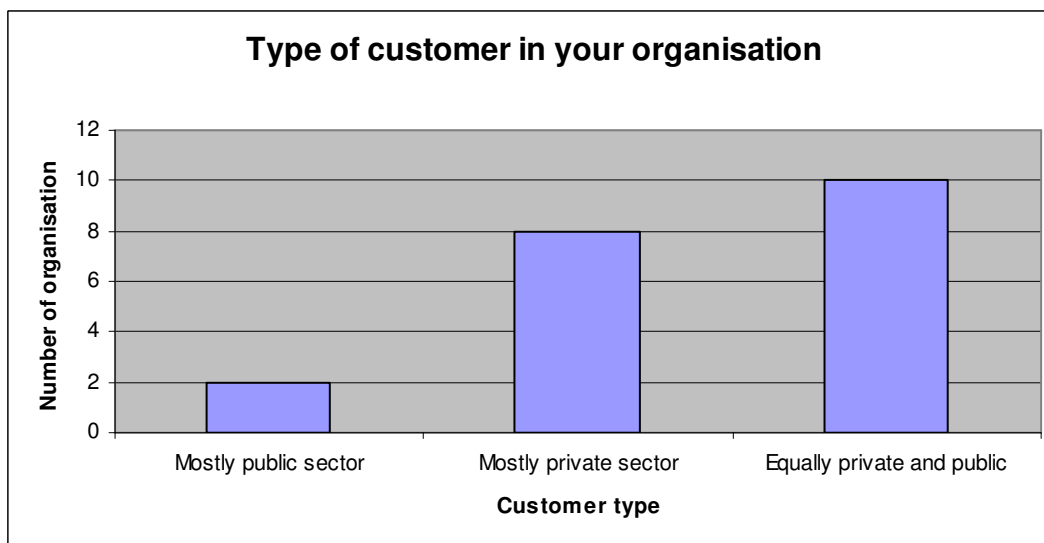


Figure 32 Overview organisations type of customer

Figure 33 displays organisations degree of software development in Norway. 50% of the organisations have “little” or “some” of the software development in Norway, while 45% have “a great deal” or all.

Nothing: 5%

Little: 30%

Some: 20%

A great deal: 15%

Everything: 30%

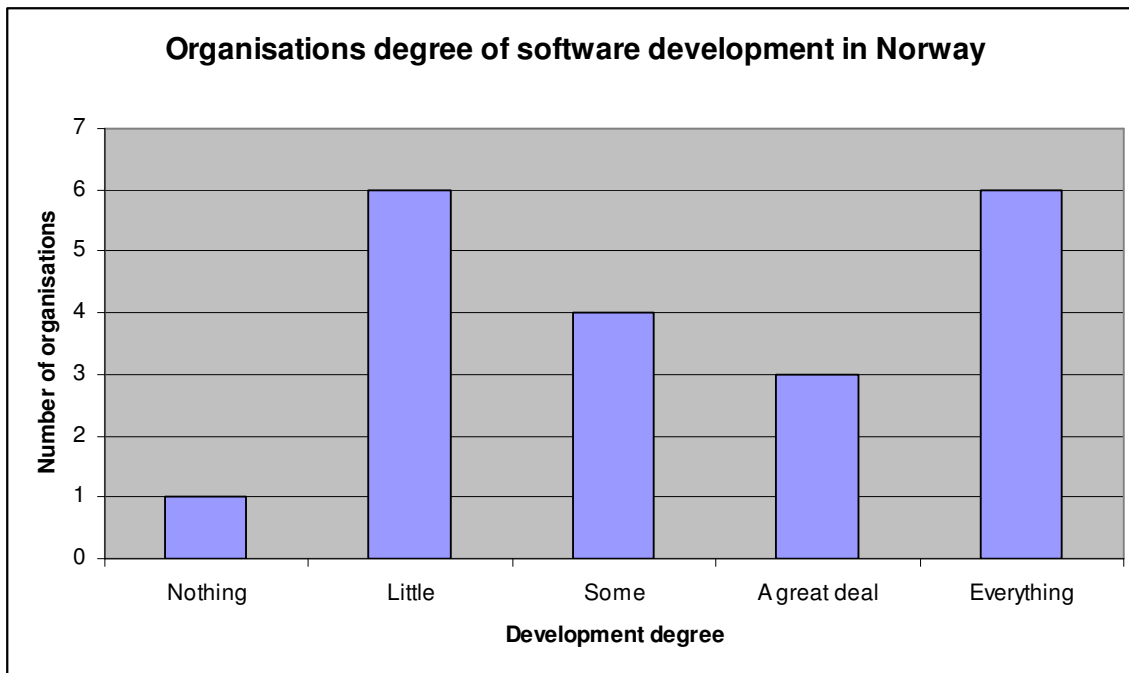


Figure 33 Overview organisations degree of software development

7.2.2 Organisations’ opinions on the use of IT-security standards

This section contains the result of finding out the organisations’ view of IT-security standards. To collect necessary information a list of propositions about organisations’ use of standards were prepared. The organisations were asked to rank their degree of agreement on each proposition. The result is given in Figure 34 and Figure 35.

The two figures show a small dominance of agreement of the propositions among the organisations.

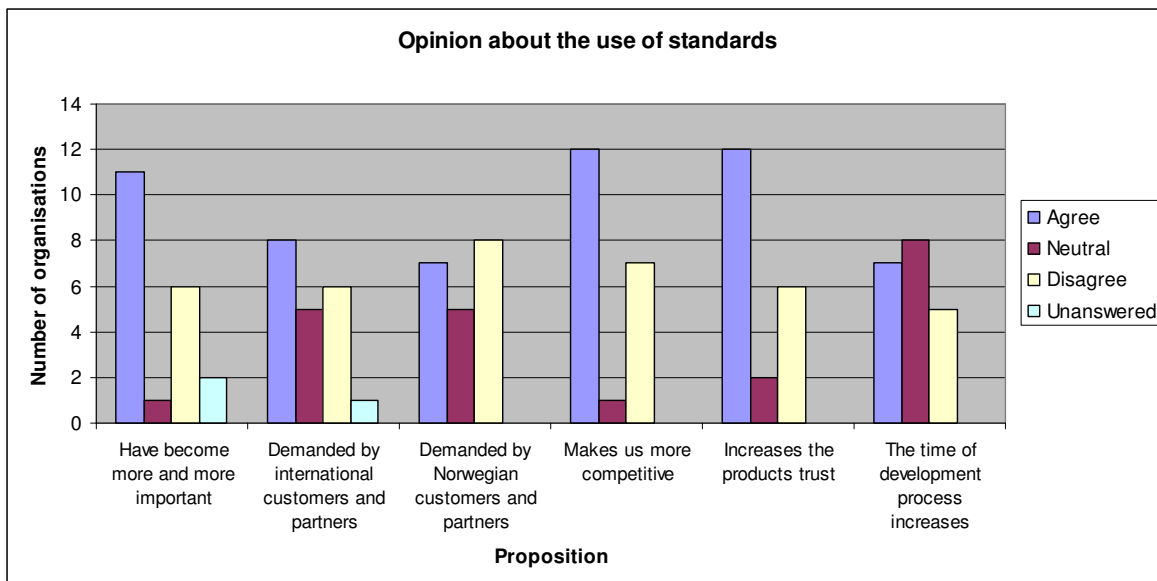


Figure 34 Opinion about use of standards 1

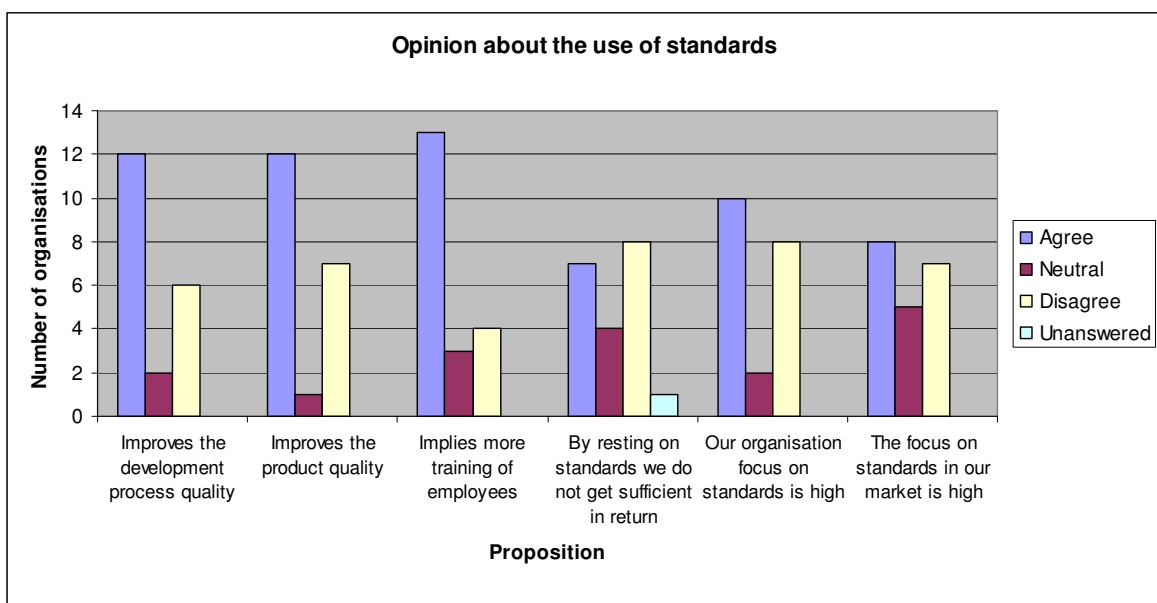


Figure 35 Opinion about use of standards 2

7.2.3 Organisations use of IT-security standards

This section contains the results of locating organisations' use and knowledge about known IT-security standards, whether they follow them or are certified by to them. The purpose was to investigate if organisations have knowledge about the standards on which CORAS is based. Most standards are not concerned with certification. Two results are presented; organisations use of standards to follow, and organisations use of certification standards.

Figure 36 gives the results from the use of standards organisations can follow. The figure indicates that most of the organisations are not familiar with any of the standards. The exception is the ISO 17779 (ISO 27002) standard more than half of the organisations follow this standard. Figure 37 presents an alternative view by adding the number of organisations that have heard of the standard to the number of organisations that follow it. Information of each of the standards represented is given in the questionnaire in Appendix B.

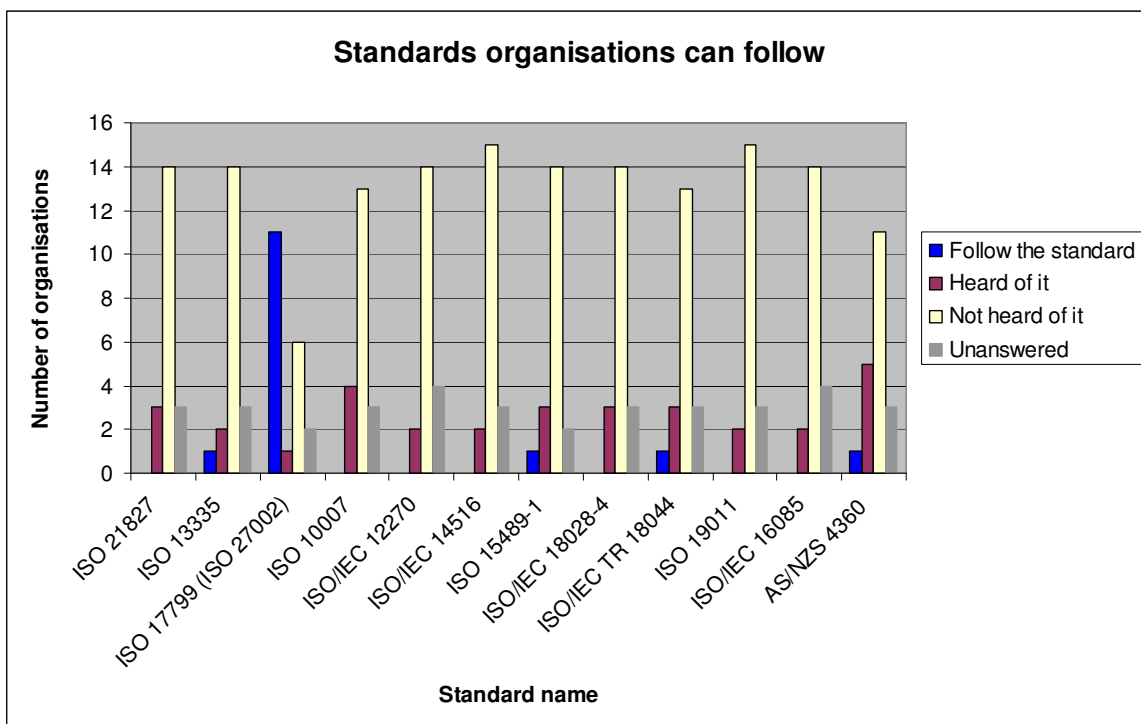


Figure 36 Organisations use of standards to follow

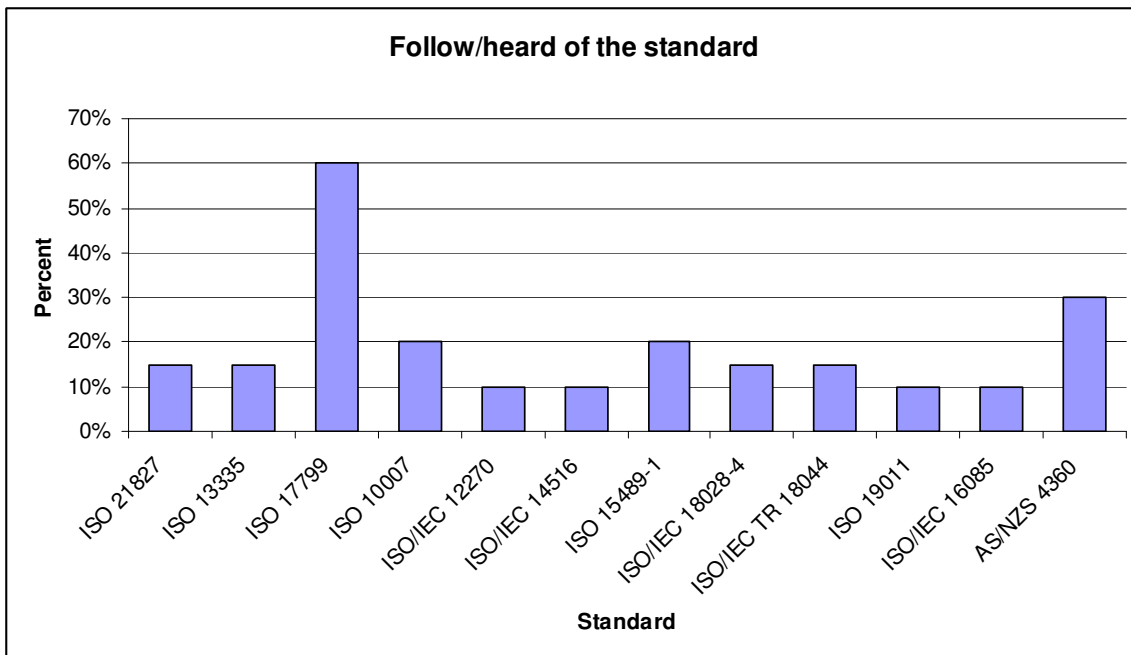


Figure 37 Percent degree on organisations follow/heard of the standards

Figure 38 displays possible certification standards. The questionnaire leaved out an opportunity “heard of it”. This may be the reason for the several unanswered results. Some of the organisations had created their own alternative “Heard of it”. This option is included in the figure.

The alternatives “We are certified”, “Going to be certified”, “Not certified, but use it as a basis” and “Heard of it” were merged. The result is displayed in Figure 39. It should be kept in mind that the result would probably be different if the missing alternative had existed in the questionnaire.

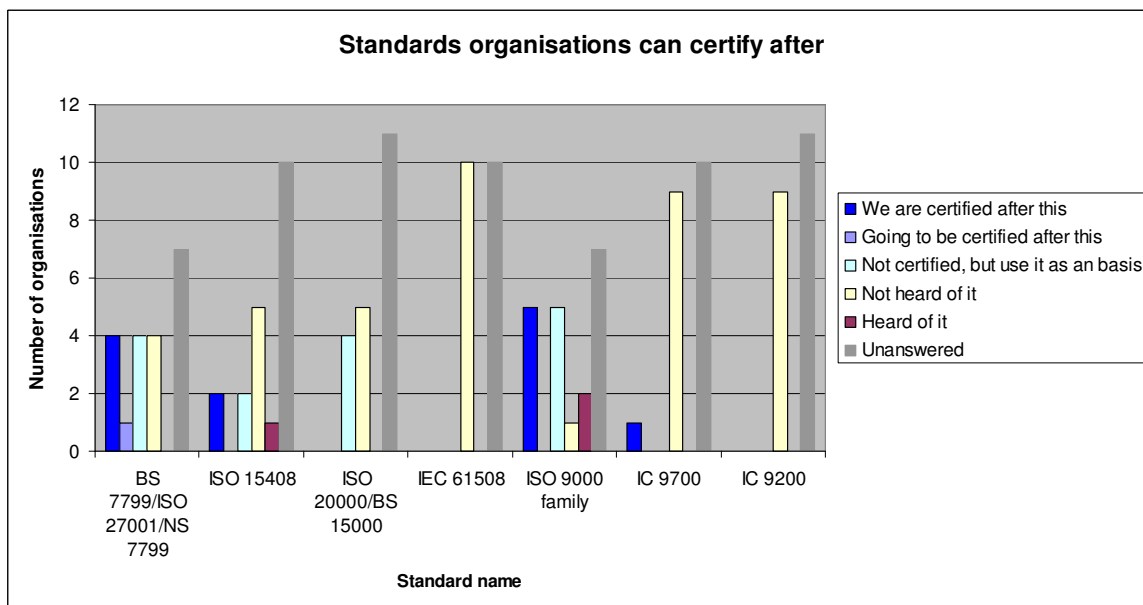


Figure 38 Organisations use of standards for certification

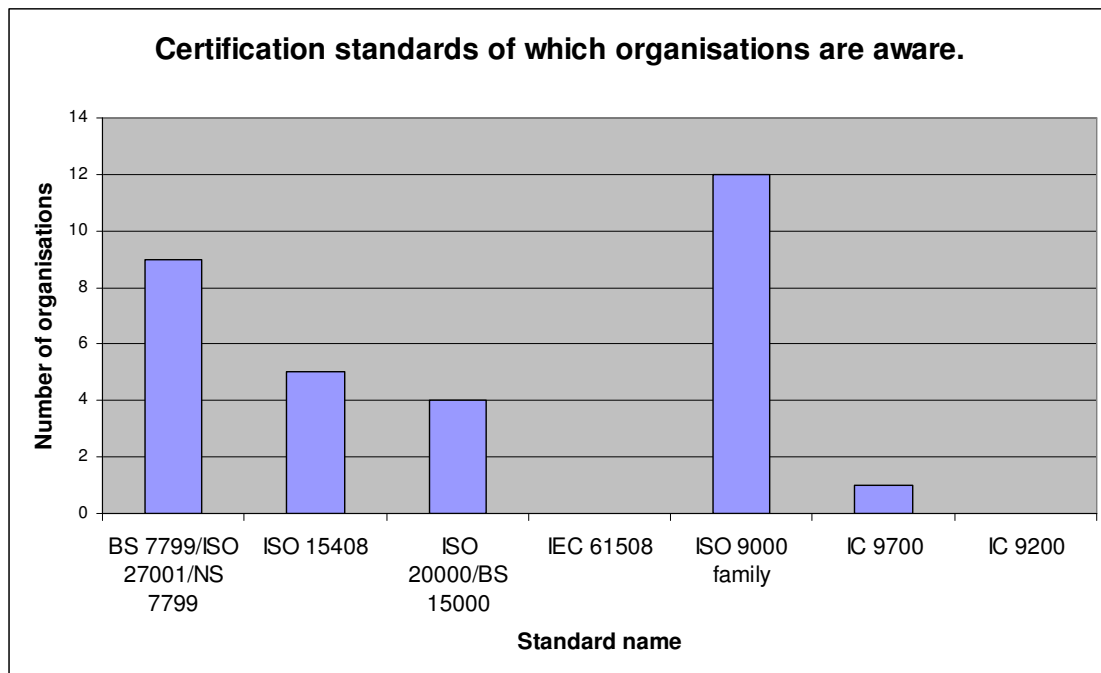


Figure 39 Certification standards of which organisations are familiar with

7.3 Evaluation of the It-security standard survey results

Based on the previous results the hypotheses from chapter 5.2 are validated. There were totally twenty organisations participating in the survey. Most of the organisations were large and private⁶. Half of the organisations' customers were evenly distributed between private and public sector, while 40% had only customer from the private sector.

HYPOTHESIS 6 The CORAS framework is based on standards already in use among organisations

- The majority of organisations follow the AS/NZS 4360 standard
- The majority of organisations are familiar with the ISO 17799 standard
- The majority of organisations are familiar with the ISO 13335 standard
- The majority of organisations are familiar with the IEC 61508 standard

The majority of organisations follow the AS/NZS 4360 standard. The AS/NZS 4360 standard is widely integrated in the CORAS framework. The standard has been available for quite long since it was first published in 1995 [16]. From the results we can see that 30 % have heard of the standard where one of the organisations

⁶ Of the selection 85% were private organisations and 50% of the organisations had more than three hundred employees.

follows the standard. As shown in this survey the AS/NZS 4360 standard, is the second most known among of the twelve standards (Figure 36). Only one of the twenty organisations follows this standard. It can not be concluded that most organisations follow it. However, this standard is the second most known standard according to this survey. Therefore, we may assume that that this standard is one of the best known among available IT-security standards.

The majority of organisations follow the ISO 17799 standard. The CORAS terminology takes its basis partly in the ISO 17799 standard. In the survey there were 60 % (55% follows it) who either follow or have heard of the standard (Figure 37). This is more than half of the organisations that participated in the survey. Based on this survey it can be assumed that organisations are familiar with the ISO 17799 standard.

The majority of organisations are familiar with the ISO 13335 standard. The ISO 13335 standard is one of the standards the CORAS terminology is based on. In the result 15 % of the organisations have either heard of the ISO 13335 standard or follow it (Figure 37). Thus it is not reasonable to believe that organisations are familiar with the standard.

The majority of organisations are familiar with the IEC 61508 standard. The IEC 61508 is standard used for certification. As displayed in Figure 38, ten (50 %) of the organisations did not answer the question. This may be because the missing option “heard of it”. Thus it is difficult to decide whether organisations are familiar with the standard. The other ten organisations had not heard of the standard. Therefore it can be assumed that at least half of the organisations had not heard of the standard. Therefore according to this survey not a much known standard.

Conclusion. Whether the CORAS framework is based on standards used in practice among organisations is difficult to answer. The selection of twenty organisations is not enough to conclude. But from this survey there can be affirmed that at least one of the four IT-security standards CORAS is based on is well known among organisations. This is the ISO 17799. The AS/NZS 4360 standard is also known, but it is not a standard organisations use to follow.

To summarise, the organisations in this survey are not particularly familiar with standards. Since only one of the four standards, on which CORAS is based, were used in practice it can not be concluded that the standards CORAS is based on are the standards used in practice. Generally speaking, organisations do not know of many standards (Figure 36 and Figure 38).

HYPOTHESIS 7 There is a need for good IT-security standards among organisations

- The use of IT-security standards makes the organisation more competitive
- IT-security standards are required by the organisations' clients
- Use of IT-security standards will increase the efficiency in the development process

- The use of standards improves the product quality and the development process quality
- The Use of standards increases the customers trust in products
- Organisations have much focus on standards both in the organisation and in the market

The use of IT-security standards makes the organisation more competitive. From the result in Figure 34 60 % of the organisations agreed in that the use of standards make them more competitive, while 35 % disagreed. Generally this survey showed that organisations believe the use of standards makes them more competitive.

IT-security standards are required by the organisations' clients. The organisations may have both Norwegian and international clients. Would the Norwegian and international clients have different requirement and demand according to the organisations use of IT-security standard? The result in Figure 34 shows that 40 % of the international customers demand use of standards and it is not demanded by 30 %. While 35 % of the Norwegian clients demand use of standards and 40 % do not demand it. 25 % of the organisations could not decide if the customers demand use of standards.

To summarise almost half of the organisations had customers that demanded use of standards, but we do not know whether it is required by the customers.

Use of IT-security standards will increase the efficiency in the development process. The result in Figure 34 shows that 35 % of the organisation believed that the time of the development process increases if the organisation uses standards, while 25 % disagreed. The majority of the organisation believed that the time of the development process would increase. This means that they probably do not believe that the efficiency in the development process will increase.

The use of standards improves the product quality and the development process quality. In Figure 35 60 % of the organisations answered that the use of standards improved the development process quality and 30 % disagreed. It also shows that twelve 60 % believed that the products quality will be improved while 35 % disagreed. More than half of the organisations agreed in both propositions. Thus this survey shows that organisations believe the use of standards improves the product quality and the development process quality.

The Use of standards increases the customers trust in products. In Figure 34 60 % of the organisations believed that the use of standards increased the product trust, while 30 % disagreed. Thus most of the organisations believed that use of standard would increase the product trust.

Organisations have much focus on standards both in the organisation and in the market. In Figure 35 it seems that the focus on use of standards and in the

organisation is quite even⁷. It can not be assumed that organisations have much focus on standards in the market and in the organisation.

Conclusion. Is there a need for good IT-security standards among organisations? A decisive element that decides this is the organisations clients demand and require for quality systems. From the results most organisations believe that the use of standard increases the products trust, quality and development process quality. Thus it is not much doubt that use of good standards improves the product. But organisations would probably not use it before their clients demand it. Half of the organisations have customers that demand the use of standards, but they probably do not require it. Another element that probably has influence on the need for standard is money. As presented in Figure 35 65 % of the organisations believed that the use of standards implies more training of the employees (and time is money for organisations).

This survey has shown that it is various whether organisations follow or are certified by standards. Most of the standards presented in the questionnaire were unknown for the organisations and only one, ISO 17799, were followed by more than half of the organisations. Beyond half of the organisations answered that the use of standards becomes more and more important. A require for IT-security standard would increase because organisations focus on security have become more widespread. The need for good standards is various among the organisation. As long as use of standards is not demanded by the organisations customers, the use of standards would probably not increase in the future.

To summarise the need for good IT-security standards is increasing. It will become more important in the future. At present there it is probably only required by the security critical organisations.

⁷ 50 % of the organisations have a high focus on use of standards in the organisations while 40 % do not and 40 % focus on the use of standards in the market, while seven 35 % do not.

Chapter 8

Discussion

The aim of this chapter is to evaluate whether we have managed to fulfil success criteria given in Chapter 3. For simplicity they are repeated below:

THE THESIS SUCCESS CRITERIA:

- The field trial in Agresso is successful if we are able to evaluate CORAS with respect to whether:
 - The CORAS UML profile supports and simplifies the analysis process
 - The CORAS tool increases the quality and efficiency of an analysis
 - Use of the CORAS RMP improves the quality of the organisations' system
- The IT-security standard survey is successful if we are able to evaluate whether:
 - CORAS is based on the standards most commonly used in practice
 - There is an increasing use and need for IT-security standards

The chapter is structured after the thesis success criteria.

8.1 The CORAS field trial in Agresso – A success?

This section discusses the success criteria for the field trial in Agresso. Below follows a discussion of the evaluation from Chapter 6.2.3, Chapter 6.3.2 and Chapter 6.4.3. The sections include a discussion of the tested hypotheses, the hypotheses limitation and a conclusion of the success criterion discussed.

8.1.1 The CORAS UML profile supports and simplifies the analysis process

The intention with the CORAS UML profile is to simplify and support the analysis process. This includes CORAS UML profile to be comprehensible for all parts involved in an analysis. During an analysis process risk terms, icons and different types of diagrams are used with the aim to support the documentation and simplify the understanding of the system. The evaluation that contributes to this discussion is given in Section 6.2.3.

8.1.1.1 The tested hypotheses

There were formulated two hypotheses according to the CORAS UML profile. The main findings of the hypotheses are given below.

HYPOTHESIS 1: Terms and icons used in CORAS are intelligible for all parts involved in the analysis. According to the analysis team it appears from the result that the terms and icons used in CORAS are intelligible for all parts involved in the analysis. The results were satisfying and all the sub-statements were answered.

HYPOTHESIS 2: The unwanted incidents and treatment diagrams are easy to understand and support the analysis process. Because of the lacking results not all of the hypothesis sub-statements were fully answered. We can not fully verify that the unwanted incidents and treatment diagrams are simple to understand and support the analysis process. Anyway it seems like the participants had no problem understanding the models. The result also showed that the models improved the communication and thus supported the analysis process.

These hypotheses only partly answer whether the CORAS UML profile supports and simplifies the analysis process. There are three main purposes with the use of CORAS UML profile; support the communication, document risks, reuse of risks. The two hypotheses above only covered whether the profile were comprehensible and supported the communication. The process answering all the three purposes would require a longer research. As we see from the security analysis report in Appendix D, the diagrams were also used to document the results. In addition the organisation can use this experience and report in other similar analyses. If the report is easy to read and understand it will increase the chance of reuse. But there exist no evidence whether the analysis participants believed the documentation were good and would reuse it in other cases.

8.1.1.2 Limitations

The verification of Hypothesis 1 and Hypothesis 2 has some limitations. We can not decide that the hypotheses hold in all cases. We can only verify that it holds in this case and for this analysis team.

In the evaluation of Hypothesis 1 the results propose that the team believed the icons and terms were simple to understand. The result only contained terms and icons used in this analysis not all the terms and icons CORAS suggest to use. Thus this statement is limited to hold for the terms and icons used in this analysis.

A limitation to the Hypothesis 2 that could have influence on the result is the analyst leader's' ability to communicate and explain the models. A vague explanation of the CORAS's diagrams and lack of explanation may affect the analysis. The terms should be explained to clarify the meaning between the analysis participants. The analysis started with a short introduction to CORAS with explanation of CORAS's related terms and icons. The results may be different if CORAS was not introduced. Another issue is whether the participants' knowledge of UML will affect the analysis participants understanding of CORAS diagrams.

Finally the number of limitations that need to be considered:

- The result of the participants understanding of the terms and icons only holds for the concepts used in this analysis
- The participants knowledge of UML
- The analyst leaders ability to explain the models

8.1.1.3 Conclusion

In general we believe that use of models in an analysis is good. It is easier for participants to point out their viewpoints in models. The question is whether the CORAS UML profile is good enough to support and simplify the analysis process. CORAS inherits much from the UML modelling language and suggest using UML models in addition to the CORAS specific models. The use of UML is increasing. The understanding of the diagrams can be difficult for people that are not familiar with the CORAS diagrams. We do not know the CORAS customers and their background of UML. Therefore an idea is to simplify the UML models to fit all possible analysis participants. Table 12 in Chapter 6.2.1.3 shows that one of the analysis participants find it difficult to understand the CORAS diagrams while another find the diagrams mostly self-explanatory. It could be due to their knowledge of UML.

We can not verify whether the CORAS UML profile supports and simplifies the analysis process. The Hypothesis 1 holds in this case. The Hypothesis 2 remains unanswered because of the lack of result. In addition there could be formulated other hypotheses in order to be able to verify or falsify the success criterion.

8.1.2 The CORAS tool increases the quality and efficiency of an analysis

The purpose of the CORAS tool is to assist the analyst leader during an analysis, both in documentation and to efficiency the process. The tool was used by the analyst leader as a guide and to document the result. The evaluation that contributes to this discussion is given in Section 6.3.2.

8.1.2.1 The tested hypotheses

In order to evaluate the CORAS tool there were formulated one hypothesis, Hypothesis 3. The main findings of this hypothesis are presented below.

HYPOTHESIS 3: The CORAS tool improves the analysis and increase the efficient of the analysis. This hypothesis with the belonging sub-statements was fully answered. The evaluation verifies that the tool does not satisfy its purpose. The intention is good but there exist many errors and lacks (see Table 16) that need to be fixed. Thus the CORAS tool version 2.0.1 is not supporting the analysis process. Instead of increase the efficiency of the analysis process, the tool rather slows it down. The many errors and deficiencies prevented the performance.

The analysis report created from the tool could not be used. The entire security analysis report document (in Appendix D) had to be reformatted which delayed the delivery of the report.

8.1.2.2 Limitations

The results and evaluation of the tool was performed by one person, the analyst leader. Different people with different background would differently judge the tool. In order to verify the result the tool should be tested by several persons. The tool should have larger scope of people to test it before decide the final conclusion. To get as good result as possible the tool should during the development process be eventually tested.

8.1.2.3 Conclusion

The idea of a tool to support an analysis is brilliant. Analysis distinguishes from each other. The people involved and the kind of system would lead the analyses in different directions. Thus the tool has to fit the needs of each analysis. If the analysis team want to add own specific models to the documentation the tool should support this. In addition if it is a need to change one of the tables used, the tool should also support this.

Sometimes people desire only to draw arrows and boxes, thus the CORAS editor should fit this purpose. Adding own icons to the editor should be appended as well. In addition allow to rearrange the order of the tables, or leave out some of the tables or drawings when creating the report.

There are a lot of actions that can be performed to improve a tool. The most important thing is probably to make people use it. Some of the most important criteria for make people use the tool is that it has to be flexible, easy to learn and use.

The CORAS tool did not satisfy the analyst leader's expectation. At this point in time, the tool does not increase the quality and efficiency of an analysis. The CORAS tool is not flexible enough and consists of many lacks and errors, but it is easy to learn and use (according to the analyst leader). There is no need to formulate additional hypotheses to further answer the success criterion.

8.1.3 Use of the CORAS RMP improves the quality of the organisations' system

The CORAS RMP is the guideline for identify risks. The purpose is to help organisations identify threats and vulnerabilities in their system. The main aim of CORAS is to offer a framework that would assist and support the organisation to create good quality systems. The evaluation that contributes to this discussion is given in Chapter 6.3.2.

8.1.3.1 The tested hypotheses

There were formulated two hypotheses in order to evaluate parts of the risk management process. The main findings of these hypotheses are given below.

HYPOTHESIS 4: The CORAS customer was pleased and would continue use CORAS in the future. The hypothesis could not be verified with confidence, because the lacking results. The hypothesis sub-statement could not be directly related to the hypothesis and if the sub-statement was answered or not, we could not verify the hypothesis. Therefore to answer the hypothesis, the sub-statements should be reformulated.

The process of perform an analysis and at the same time accomplish a research of it is time consuming. Therefore it is not realistic to get an answer to this hypothesis. The result of the analysis would be carefully discussed by Agresso in order to decide whether to continue using CORAS.

HYPOTHESIS 5 The result and the accomplishment of the analysis meetings were good. In order to fully verify this hypothesis it probably could be gathered more information. The result showed that the communication of the meeting was good and there were an appropriate number of participants. In order to answer and improve the hypothesis it should be considered whether the number of meetings was appropriate, the meetings results were satisfying or if the efficiency of the analysis meetings were good. The general accomplishment of the meetings was satisfying. It was the accomplishment of these meetings that lead to the security analysis result (Appendix D).

There should be formulated additional hypotheses that contribute answering whether the CORAS RMP improves the quality of the organisations system. There are several factors that could be related to the quality of a system, not only whether the analysis meetings were good and whether the organisation would continue used CORAS in the future. Probably the most important thing before performing an analysis is to investigate the organisation expectations of a quality system.

The analysis report gives a good documentation of the PunchOut functionality. For an organisation like Agresso it is important of good documentation that will contribute for new developers to easy understand earlier work accomplished on the system. Good documentation could give PunchOut a higher quality in the future development. Thus CORAS may have contributed to improve the quality of the PunchOut functionality's next version.

Even if we could not fully answer the success criterion of whether CORAS improves the quality of the system, the result of the analysis shows that there exist some risks with the functionality. If the developers of PunchOut treat these risks the functionality is improved. Thus CORAS has supported in improving the quality.

8.1.3.2 Limitations

In addition to IT-systems, CORAS could also be involved in other critical systems. There is a possibility that CORAS would be significant in one system, but poor in other systems. We need to gain knowledge of different types of systems and perform different types of analyses. This thesis is limited to one IT-system.

The results from Figure 28 indicate that in general the analysis team believed the analysis were efficiency. A limitation to this could be that we do not know how each participant defines efficiency. Do they think of efficiency according to other analyses or is it according to the entire development process or is it according to their expectations of how efficient the analysis should be. The definition of the efficiency in the analysis should be emphasized.

8.1.3.3 Conclusion

There are many factors in an analysis that plays a role when improving the quality of a system. The main purpose is to be able to find all risks in a system and let the organisation decide whether to solve these risks. This does not only depend on the risk analysis method used. In the cooperation with the organisation, the analyst leader's ability to disseminate messages and direct the team into right track plays an important role of the ability to find risks. To guide the analyst leader it could be useful to have a guideline with tips and tricks in addition to the already available checklists.

It is not possible to remember all earlier analyses. Thus it is important to have a good experience library where the analyst leader (and the team?) can easily take advantage of similar cases.

There are several factors that decide the quality of a product. In order to improve the system quality we need to find these factors. We need to find out the organisations opinion of quality.

In order to answer the success criterion it should be considered the factors that improve the quality of the CORAS risk management process and the factors that improve the quality of a system.

The result and evaluation of the CORAS RMP is not verified. It is not possible to verify whether the use of CORAS RMP improves the quality of the organisations system, not even in the AGRESSO POF. In order to verify this success criterion there should exist additional results. With basis in the analysis report we can only assume that CORAS improves the quality of the PunchOut functionality.

8.2 The IT-security survey investigation – A success?

This section discusses the investigation of CORAS according to IT-security standards and the use of IT-security standards. The evaluation that contributes to this discussion is given in Chapter 7.3.

8.2.1 CORAS is based on the standards most commonly used in practice

The CORAS inherits much from IT-security standards. If organisations are known with the standards CORAS is based on, it is a probability that they know the concepts used in the CORAS. This section discussed the evaluation of the CORAS is based on known and used standards.

8.2.1.1 The tested hypotheses

There was formulated one hypothesis in order to answer whether the standards used in the CORAS are the same as used in practice.

HYPOTHESIS 6 The CORAS framework is based on standards already in use among organisations. Generally the IT-security standards in the questionnaire were not known. Among the four IT-security standards CORAS is based on, two of the standards stand out as more known. The ISO 17799 standard, were used by more than half of the organisations. The AS/NZS 4360 standard were also known among several of the organisation, but not used.

8.2.1.2 Limitations

A number of limitations should to be considered. A limit is that the scope of organisations participated in the survey was too small to draw finite conclusion. In order to get significant results the scope should be more than twenty organisations.

Among twenty participated organisations most were private. The result could be different with a dominance of public organisations. The majority of the organisations were large⁸. A larger organisation is usually more vulnerable than small organisation, e.g. because the possibility for unfaithful employees increases with the organisation size. This also could have affected the result.

Would the organisations type of customers affect organisation decision to IT-security standards? If customers do not demand organisations to use IT-security standards, organisations may not focus on using standards. E.g. a hospital may have more strict requirement to IT-security and risk management than an organisation where an security breach do not affect the organisation or the customer. Another factor that may have influence of the result is if the organisation is international or have international customers. Would foreign countries have strict requirements to the use of standards?

In order to limit the results the questionnaire should be limited with:

- Organisations type
- Organisations size
- Organisations customer
- Internationalisation

8.2.1.3 Conclusion

The use of standards in organisations seems to be rare. Among the nineteen IT-security standards mentioned in the questionnaire only a minority is used by the organisations. This indicates that just a few IT-security standards are widely used, but the most used is (according to the survey) ISO 17799, a standard CORAS is based on. The limitations of this survey is generally restricted to private organisations with more than or equal to three hundred employees. If we accomplish a survey with limited to small, public organisations, would the outcome be different?

The ISO 17799 is not the standard CORAS inherits most from. It is the Australian standard AS/NZS 4360. The survey indicates that most organisations have not heard of this standard. Among the twenty organisations only one organisation follow the standard. The AS/NZS 4360 standard should have been more known and used before we can conclude that CORAS is based on the standards most commonly used in practice.

⁸ More or equal to three-hundred employees

8.2.2 There is an increasing use and need for IT-security standards

Even if it does not exist any interest or need for IT-security standards at present, there may be in the future. This section discusses the evaluation of whether there is an increasing use and need for such standards (presented in 7.3).

8.2.2.1 The tested hypotheses

There was formulated one hypothesis to answer if there is an increasing use of IT-security standards.

HYPOTHESIS 7 There is a need for good IT-security standards among organisations. According to the evaluation there is an increasing need for IT-security standards, but at present there are probably most used by organisations that require strong security (e.g. the health sector). Almost half of the organisations had customers that demand use of standards. Although the organisations did not use the IT-security standards, but they saw the benefit of using standards.

In order to answer the success criteria there should be added another hypothesis. It does not clearly appear that there is an increasing use of IT-security standards. A new formulated hypothesis should contain whether the organisations intend to follow IT-security standards in the future.

8.2.2.2 Limitations

The limitation of this result is the same as the limitations described in Section 8.2.1.2.

8.2.2.3 Conclusion

The need for secure system is increasing. The market gets more vulnerable for attackers (both unfaithful employees and competitors). Thus it is reasonable to believe that organisations look for security measure to protect their system. One measure could be to follow or use IT-security standards that will result in more use of IT-security standards. Use of standards in a short-term is probably expensive, but in the long-term it will be worthy. Most of the organisations believed that use of standards would increase the organisations cost in time and training the employees. This indicates that organisations seem to think more in short-terms.

Chapter 9

Further work

This chapter gives the recommendation for further work. In order to bring the experience of this research further, it will be suggested modifications to each part of investigation and additional suggestion to improve and continue the work of this thesis.

9.1 The CORAS framework

This section recommends further work of the CORAS UML profile, the CORAS tool and the CORAS RMP.

9.1.1 The CORAS UML profile

The Hypothesis 2 was not fully answered. To continue the work it should be answered. In addition to the two hypotheses formulated it is recommended to formulate a third hypothesis in order to investigate whether the CORAS UML profile gives good documentation and supports reuse in a good way. To continue the investigation of whether the CORAS UML profile supports and simplifies the analysis process there are several factors that could be considered. Thus the further research might be amended by observing:

- Whether the analysis participants knowledge of UML affect the understanding of the models used in the analysis.
- Whether the analyst leader's explanation of the CORAS UML profile affected the understanding.
- Find out what makes the CORAS's diagrams and icons difficult to understand and what makes them simple to understand.

9.1.2 The CORAS tool

The CORAS tool should be tested continuous with releases of new versions. The tool should also be tested by several potential users with different needs and requirements. Before the adjustment of the deficiencies and errors found in this thesis, the results need to be tested by a larger scope of people. The same observations as used in this thesis could be used. The observations for further research should be:

- The learning process
- The use of the CORAS methodology guide that follows the tool
- The use of the tools functionalities (tables, diagram editor, report generator)

9.1.3 The CORAS risk management process

It is difficult to test whether the CORAS RMP improves the quality of the organisations system. In order to complete the investigation in this thesis the formulated hypotheses of CORAS RMP need to be amended. In addition there should be formulated new hypotheses. The new formulated hypotheses should consider factors that contribute to make a quality system. For instance answer whether the CORAS RMP contributed to:

- Find any critical risks
- Increase the system performance
- Prevent unauthorized to receive confidential information
- Preserve the system integrity
- Preserve a available system
- Achieve good system documentation

Performing an analysis require finding out the organisation's intention with the analysis. What factors increases the quality of the system?

The CORAS RMP will not achieve a satisfying result if the elements (e.g. analysis meetings, team composition) in the process were not satisfactory.

Thus future work might investigate:

- What factors improve a system?
- Investigate whether the elements in an analysis will improve the risk management process

In addition, the CORAS RMP should be performed on different types of systems.

9.2 CORAS according to IT-security standards

This section recommends further work to the survey of CORAS according to IT-security standards.

In the future there should be accomplished several surveys to support the evaluation of this research. The same experience with use of questionnaire could be used. The questionnaire (Appendix B) should be improved by adding an option, “har hørt om den”, to the last table in the questionnaire (see Table 27)⁹.

Standarder man kan sertifiseres etter:	Vi er sertifisert etter den	Vi skal sertifiseres etter den	Vi er ikke sertifisert, men baserer oss på den likevel	Har ikke hørt om den
BS 7799 / ISO 27001 / NS 7799				
ISO 15408 – The Common Criteria				
ISO 20000/BS 15000 - IT service management				
IEC 61508				
ISO 9000 family				
IC 9700 Enterprise Certification				
IC 9200 Small business Certification				

Table 27 Missing option in questionnaire

For possible future study limitations to the result should be considered. The scope of organisations could be categorised into; organisation size, type, customer, internationalisation, and the degree of software development. If we manage to gather result divided after these categories we can compare each result to see whether these factors influence the organisations need and use of IT-security standards. Whether there are different opinions about standards among organisations in the public sector than the private sector might be interesting to see. To summarise, the limits to consider in further work:

- Organisations size
- Organisations type (public, private, other)
- Internationalisation
- Organisations customer
- The degree of software development (in Norway and in foreign countries)

A challenge in the further process is to be able to gather information from organisations. The process of gathering questionnaire results is time consuming. The investigator should be prepared to an early start.

⁹ The Table 27 is a part of the questionnaire that were performed and written in Norwegian, thus it is not translated to English and have different formatting.

Chapter 10

Conclusion

This chapter presents a short summary of the thesis and the main result of evaluation.

10.1 Summary

The goal of the research was to continue the research of CORAS with the purpose of evaluate and improve the CORAS framework. The research consisted of two main investigations:

- Investigate parts of the CORAS framework
- Investigate organisations use and need of IT-security standards

In order to limit the research there were created thesis success criteria. The main purpose of this research was to evaluate these success criteria. To be able to answer the success criteria a number of hypotheses were formulated. This paper has given an account for the evaluation of these hypotheses and a discussion of whether the thesis success criteria are fulfilled. The hypotheses were compared with evidence from two investigations:

- *A field trial in the Agresso organisation:* A full security analysis of industrial scale was accomplished in the Agresso organisation. During the analysis results were collected.
- *An IT-security standards survey:* Twenty organisations answered a questionnaire about their relations to IT-security standards

10.2 Results

The result of the discussion and evaluation of the two investigations are presented in the table below. Each investigation part summarise the main result, limitation and suggested further work.

The CORAS UML profile	Results	The result shows that in general there are no particular problem understanding the CORAS UML profile or any terms and icons used within an analysis.
	Limitations	Will the participant's knowledge of UML have influence on the understanding of CORAS UML profile?
		Will the analyst leader's ability to explain the models affect the understanding of CORAS UML profile?
	Further Work	To investigate what influence the understanding of the CORAS UML profile.
The CORAS tool	Results	The result shows that the tool is not satisfying. There exist several errors and deficiency. But if these flaws are corrected the tool would probably be satisfying.
	Limitation	Will other analyst leaders have the same experience as this thesis analyst leader?
	Further Work	Test the errors and deficiencies found. Perform the same test on each version of CORAS.
The CORAS RMP	Results	The results indicate that there were difficult to decide whether CORAS RMP improves the quality of the organisation's system. To be able to consider whether CORAS RMP increases the quality there is need for several hypotheses that cover all the aspects of a quality system and whether these aspects were improved by using CORAS RMP.
		The security analysis shows that it is possible to perform a security analysis with the CORAS RMP and get satisfying results.
	Limitation	Is CORAS equally suited for other than IT systems?
	Further Work	Investigate what factors improve a system.
		Investigate what elements in the analysis that will contribute to improve the analysis process.
CORAS according to	Results	The uses of IT-security standards among the

IT-security standards		twenty participated organisations are rare. The standards that are most commonly used by organisations CORAS are based on these standards.
		Organisations are more aware of security risks. But still they believe that there use of IT-security standards increases the expenses in the organisation.
	Limitation	Will the organisation type and size influence the organisations use of standard?
		Will the organisations' customer affect the organisations use of standards?
		Will organisations degree of contact with foreign countries (internationalisation) affect the use of standards?
Further work	Perform the same survey among a number of organisations and emphasise the limitations.	

Table 28 Main result of the investigations

These results showed that we were able to find improvements with CORAS which brings the investigation of CORAS to the next level.

The aim of this thesis was to answer whether 1)the CORAS field trial was a success and 2) whether there is a need for such a guideline in the future.

The CORAS field trial in Agresso a success? The analysis report showed that it was possible to use CORAS to complete a security analysis in Agresso. If Agresso treat the risks found, the PunchOut functionality will be improved. Even if we were able to finish an analysis the results of the investigation show that there CORAS could be improved in order to achieve good results.

Is CORAS needed among organisations in the future? The IT-security standard investigation showed that organisations are more concerned with security now than ever before. In addition, the evaluation shows that there is an increasing need for tools that will guide organisations in improving the quality of their system.

This thesis has shown that CORAS was successful in an organisation and that it is reasonable to believe that there is a need for good security guidelines, such as CORAS, in the future.

Bibliography

- [1] Mass Soldal Lund, Ida Hogganvik, Fredrik Seehusen, Ketil Stølen: “*CORAS, Risk Assessment of Security Critical Systems*”, version 1.0 (03.037 WP3 Act 3.6 D3.7)
- [2] Mass Soldal Lund, Folker den Braber, Ketil Stølen: “*Maintain results from security assessment*”, <http://coras.sourceforge.net/documents/csmr2003.pdf> , 2006-02-02
- [3] “*CORAS Integration Platform*”, <http://folk.uio.no/ketils/coras/platform-poster.pdf>, 2005-04-29.
- [4] Ketil Stølen web page, <http://folk.uio.no/ketils/>, 2006-02-02
- [5] UML web page, <http://www.uml.org/> , 2006-02-02
- [6] Securis, <http://folk.uio.no/ketils/securis/index.htm>, 2006-02-02
- [7] CORAS web page, <http://coras.sourceforge.net/>, 2006-02-02
- [8] Fredrik Vraalsen, “*CORAS vision v0,5*”, 2005-01-24, Sintef internal document.
- [9] Claes Wholin, Per Runeson, Martin Höst, Magnus C Ohlson, Björn Regnell, Anders Wesslen. Edited by Victor R. Basili, “*Experimentation in software engineering, an introduction*”, Kluwer Academic publishers, 2000
- [10] Richard L. Baskerville, “*Investigating information systems with action research*”, Georgia State University, 1999-10-19.
- [11] Felix Redmill, Morris Chudleigh, James Catmur: “*System safety: HAZOP and Software HAZOP*”, John Wiley & Sons, 1999.
- [12] Gry Brændeland, Ida Hogganvik, Fredrik Seehusen, ”*Plan for evaluation of the fourth SECURIS field trial v4*”, 2005-01-21, Sintef internal document.
- [13] Agresso R&D AS Norwegian web page, http://www.agresso.com/norway/home.asp?f=norway/overview_home.asp , 2006-02-02
- [14] Thomas R. Peltier: “*Information Security Risk Analysis*”, Auerbach publications, 2001, ISBN 0-8493-0880-1

[15] The CORAS project web page, <http://coras.sourceforge.net/documents/2002-EDOC.pdf>, 2006-02-27

[16] AS/NZS 4360 (2004) Australian / New Zealand Standard for Risk Management

[17] ISO/IEC TR 13335-1 (2001) Information Technology –Guidelines for the management of IT Security – Part1: Concepts and models for IT Security.

[18] ISO/IEC-17799-1 (2000) Information technology – Code of Practice for information security management

[19] IEC 61508 (1998-2000): Functional Safety of Electrical /Electronic/Programmable Electronic Safety-Related (E/E/PE) Systems

[20] ISO/IEC 10746 (1995): Basic reference model for open distributed processing

Appendix A

Agresso field trial surveys

A.1 Questionnaire 1

Evaluering av møte

Har du deltatt på en sikkerhets/risikoanalyse før?

Ja	
Nei	

Kjenner du til begrepene og gangen i en sikkerhets/risiko analyse?

Ja	
Delvis	
Nei	

Tror du sikkerhets analyse er nyttig?

Ja alltid	
I noen tilfeller	
Nei, aldri	
Nyttig, men koster for mye tid og penger.	
Annet:	

Synes du CORAS elementene var lette å forstå?

Ja	
Delvis	
Nei	

Kjenner du til disse begrepene i sikkerhets sammenheng?(1= Har aldri hørt begrepet, 5= Vet godt betydningen av begrepet)

	1	2	3	4	5
Aktiva					
Uønsket hendelse					
Trussel					
Sårbarhet					
Risiko					
Konfidensialitet					
Integritet					
Tilgjengelighet					

Hvor enig er du om disse påstandene for møte (1= helt uenig, 5 = helt enig)

	1	2	3	4	5
Møte var for langt					
Diskusjonene ble for lange					
Kommunikasjonen mellom deltakerene var bra					
Jeg fikk frem mine synspunkter					
Det ble for mange nye begreper					
Analyselederens lederegenskaper var gode					
Presentasjonen var oversiktlig					

Kommentarer til møte:

A.2 Interview

Intervju

- 1 Var det noen av iconene som var vanskeligere å skjønne enn andre?
- 2 Var det noen uttrykk som var vanskeligere å forstå enn andre?
- 3 Hva synes du om trussel/uønskede hendelses diagrammene?
- 4 Er diagrammene en bra måte fremstille trusler å uønskede hendelser på?
- 5 Hva synes du om kommunikasjonen på møtene?
- 6 Hva synes du om team sammensetningen? Burde det vært flere/færre?
- 7 Hva synes du om analyse leders forklaring av iconene og diagrammene? Burde den vært tidligere?
- 8 Hva synes du om risiko identifiserings møte? var det effektivt? Burde andre enn teamet være involvert?
- 9 Hvor lang tid hadde du trodd det ville ta å gjennomføre en slik analyse?
- 10 Tror du Agresso vil kunne gjenbruke resultatene fra denne analysen? Evt. Gjøre lignende analyser?

A.3 Questionnaire 2

Evaluering av analysen

Gikk analysen etter dine forventninger?

Ja	
Nei	
Delvis	
Ingen forventninger	
Kommentar	

Burde Agresso ha flere slike analyser?

Ja	
På noen prosjekter	
Nei, Det koster for mye	
Nei, Det tar for lang tid	
Vet ikke	

Hvilken fase av utviklings prosessen synes du det er mest nyttig med en sikkerhets analyse?

Alle	
Før design (starten av prosjektet)	
Før implementasjon	
Etter at mesteparten av implementasjon er ferdig	
Når systemet er ferdig	
Kommentar:	

Var analysen effektiv?

Ja	
Nei	
Delvis	
Vet ikke	
Kommentar:	

Fungerte teamet bra?

	Enig	Delvis	Uenig	Vet ikke
Kommunikasjon mellom team deltagerne var bra				
Antall deltagere i teamet var passe				
Ulike kvalifikasjonene blant team deltagerne gjorde analysen bedre				
Ulike kvalifikasjonene gjorde				

kommunikasjon vanskelig				
Det var noen som snakket betydelig mer enn andre				
Alle ble hørt				

Antall deltagere i teamet burde være (sett et kryss)

Mindre enn 5	
5-6	
7 – 9	
Variert	
Annet:	

Hvor enig er du i disse påatandene om CORAS diagrammene (1=helt uenig. 5 helt enig):

	1	2	3	4	5
Bruk av diagrammer gjorde kommunikasjonen enklere					
Den grafiske fremstillingen var vanskelig å skjønne					
Bruk av diagrammer har ingen betydning					
Bruk av diagrammer forbedrer analysen betydelig					
Bruk av diagrammer effektiviserer analysen					
Diagrammene gjør det enklere å se nye risikoer i systemet					

Kommentarer til analysen generelt: (f.eks burde noe vært gjort annerledes? Mer nøyaktig? Etc.):

Appendix B

IT-security standard questionnaire

Standarder innen IT-sikkerhet

Litt om din organisasjon:

1. Hvor mange ansatte er dere? Færre enn 25 26-100 101-300 Over 300
2. Hva slags type organisasjon? Privat Offentlig Annet
3. Hva slags kunder/samarbeidspartnere har dere?
 Mest fra offentlig sektor Mest fra privat sektor Like mange fra hver
4. I hvilken grad driver dere med softwareutvikling i Norge?
 Ingenting Lite En del Mye Alt gjøres her til lands

Hvor enig er du i disse påstandene om bruken av standarder (1=helt enig - 5=helt uenig)?

	1	2	3	4	5
Bruken av standarder har blitt mer og mer viktig					
Det er etterspurt/krav av internasjonale kunder og samarbeidspartnere					
Det er etterspurt/krav av norske kunder og samarbeidspartnere					
Det gjør oss mer konkurransedyktige					
Det gir økt tillit til produktet vårt					
Utviklingsprosessen tar lenger tid når man må basere seg på standarder					
Det bedrer kvaliteten på utviklingsprosessen					
Det bedrer kvaliteten på produktet vårt					
Standardisering innebærer ekstra opplæring av ansatte					
Man får ikke nok igjen for å basere seg på standarder					
Det er mye fokus på standarder i vår organisasjon					
Det er mye fokus på standarder i vårt marked					

En del standarder kan man sertifiseres etter, mens andre kan man følge mer som retningslinjer, i hvilken grad brukes disse standardene i din organisasjon?

Standarder man kan følge (se i listen bak for fullt navn):	Følger standarden	Har hørt om den	Har ikke hørt om den
ISO 21827			
ISO 13335			
ISO 17799 (ISO 27002)			
ISO 10007			
ISO/IEC 12207			
ISO/IEC 14516			
ISO 15489-1			
ISO/IEC 18028-4			
ISO/IEC TR 18044			
ISO 19011			
ISO/IEC 16085			
AS/NZS 4360			

Standarder man kan sertifiseres etter:	Vi er sertifisert etter den	Vi skal sertifiseres etter den	Vi er ikke sertifisert, men baserer oss på den likevel	Har ikke hørt om den
BS 7799 / ISO 27001 / NS 7799				
ISO 15408 – The Common Criteria				
ISO 20000/BS 15000 - IT service management				
IEC 61508				
ISO 9000 family				
IC 9700 Enterprise Certification				
IC 9200 Small business Certification				

Standarder:

- *ISO 21827*: Systems Security Engineering Capability Maturity Model
- *ISO 13335*: IT security management - comprises a set of guidelines for the management of IT security, focusing primarily on technical security control measures
- *ISO 17799 (ISO 27001)*: this is the Code of Practice describing a comprehensive set of information security control objectives and outlines a menu of best-practice security controls.
- *ISO 10007*: Quality management systems – Guidelines for configuration management
- *ISO/IEC 12207*: Software life cycle processes
- *ISO/IEC 14516*: Guidelines for the use and management of Trusted Third Party services
- *ISO 15489-1*: Information and documentation – Records management
- *ISO/IEC 18028-4*: Securing remote access
- *ISO/IEC TR 18044*: Information security incident management
- *ISO/IEC 16085*: Software life cycle processes - Risk management
- *AS/NZS 4360*: Australian / New Zealand Standard for Risk Management
- *ISO 19011*: Guidelines for quality and /or environmental management systems auditing

- *BS 7799 (ISO 27001/NS 7799)*: the main Information Security Management System requirements standard (specification), against which organisations will be certified.
- *ISO 15408*: Common Criteria. ISO 15408:1999 describes the Common Criteria for Information Technology Security Evaluation. Products that are evaluated against the Common Criteria have a defined level of assurance as to their information security capabilities that is recognised in most of the world.
- *ISO 20000*: - ITIL - IT Service Management - "ITIL (IT Infrastructure Library) is the most widely accepted approach to IT Service Management in the world. ITIL provides a cohesive set of best practice, drawn from the public and private sectors internationally. It is supported by a comprehensive qualifications scheme, accredited training organisations, and implementation and assessment tools. ITIL standard BS 15000 has now become ISO 20000, a two part standard.
- *ISO 9000-3*: Guidelines for the application of ISO 9001 to the development, supply and maintenance of software covers software engineering, guiding the application of ISO 9000, the quality assurance standards, to the systems development process.
- *IEC 61508*: is the international standard for electrical, electronic and programmable electronic safety related systems. It sets out the requirements for ensuring that systems are designed, implemented, operated and maintained to provide the required safety integrity level (SIL).
- *IC 9700*: is a high level business certification. As opposed to ISO 9001, the IC9700 standard certifies a companies internal processes, ethical guide measures and ensures the company operates good practice principals.
- *IC 9200*: is a popular small business certification program and is regulated by the Small Business Certification.

BS = British Standard, NS = Norsk Standard, ISO = the International Organisation for Standardisation, IEC = the International Electrotechnical Commission, IC = International Charter.

Appendix C

Introduction to the CORAS UML profile

UML is the most widely used specification language in the software industry today. A UML Profile is a refinement of the basic UML¹⁰ language targeting a more specialised application area. The CORAS project has defined a UML profile for security risk assessment. The CORAS UML profile is a UML based specification language targeting security risk assessment. It suggest to use UML to describe the target of analysis and use CORAS own graphical language to model risks. The models for security assessment are used to document the threats, unwanted incidents and risks. [2]

The CORAS UML profile is used in every step in the analysis. In the context identification process the CORAS UML Profile suggest using known UML techniques as use cases and sequence diagrams. In the risk identification process CORAS graphical language is used.

The advantages of modelling risks and threats is that it will reduce misunderstandings, graphical icons is faster to read than text and it is probably intelligible for all inexperienced parts involved.

The CORAS UML profile defines specialised diagrams and modelling elements to support the security risk analysis process and it is based on the UML standard. In the following there is given an introduction to the CORAS specific diagrams.

¹⁰ For more information about UML see <http://www.uml.org>

Unwanted incident/threat diagrams

The Table B 1 presents the threat and unwanted incidents icons used when modelling unwanted incidents.

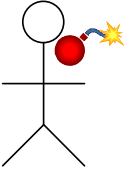
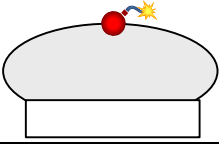



Icon	Name	Description
	Threat agent	A potential cause of an unwanted incident, which may result in harm to a system or organisation and its assets. Threat agents can be external, (e.g., hackers or viruses) or internal (e.g., system failures or disloyal employees). [2]
	Threat scenario	A description of how a threat may lead to an unwanted incident. [2]
	Unwanted incident	An undesired event that may reduce the value of an asset. [2]
	Asset	Something to which an organization directly assigns value and, hence, for which the organization requires protection. [2]
	Vulnerability	A weakness with respect to an asset or group of assets that can be exploited by one or more threats. [2]

Table B 1 CORAS threat and unwanted incidents icons

Unwanted incidents diagrams consist of threats and unwanted incidents. A threat is modelled using the threat agent and threat scenario. The threat scenario may be caused by a weakness, vulnerability, in the system that the threat agent can exploit. The threat agent (e.g. eavesdropper or malicious person) present the active part of the threat and the threat scenario is behaviour of the threat agent. A threat scenario may lead to an unwanted incident. The threats and the unwanted incidents are related to the assets they threat.

Figure B 1 illustrates an example of how to create unwanted incident diagram.

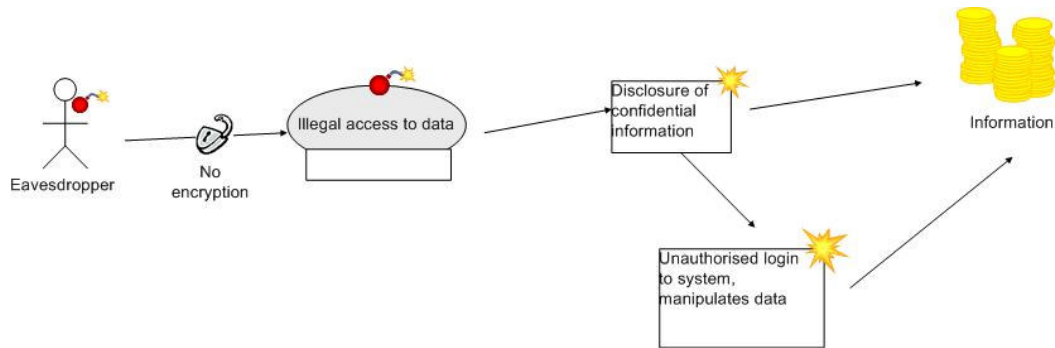


Figure B 1 Example of unwanted incident and threat diagram

Treatment diagrams

In Table B 2 there is presented a description of the treatment icons for modelling treatment diagrams.

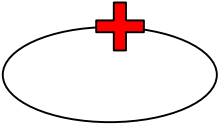

Icon	Name	Description
	Treatment	Ways of reducing the risk value of a risk or risk theme.[2]
	Treatment effect	A treatment's capability to reduce the risk value of a particular risk. [2]

Table B 2 CORAS treatment icon

The treatment diagram suggests treatment to the unwanted incidents. A treatment can be viewed as a protection against a risk. There are different categories of treatment [1]:

- Avoid the unwanted incidents
- Transfer the unwanted incident to some other target
- Reduce likelihood of the unwanted incidents
- Reduce consequence of the unwanted incidents

In Figure B 2 gives an example of how to add treatment to the unwanted incident diagram from Figure B 1.

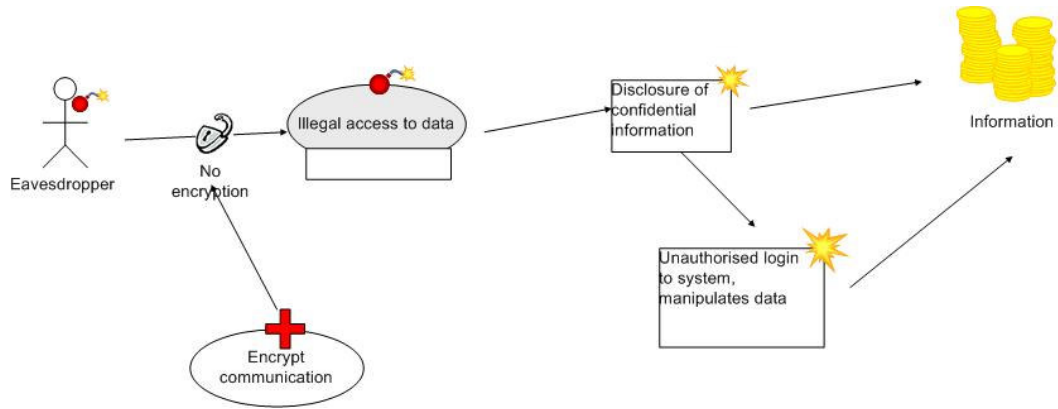


Figure B 2 Example of treatment of unwanted incident

Appendix D

The Agresso security analysis report

Security Analysis results

A security analysis of the AGRESSO PunchOut Functionality

<i>Analysis method</i>	CORAS risk management process
<i>Author</i>	Jenny B. Hougen
<i>Client</i>	Agresso R&D
<i>Date:</i>	20.04.2006
<i>Abstract</i>	This report documents the risks identified in the AGRESSO PunchOut functionality using the CORAS risk management process.

Abbreviations

Agresso:	Agresso R&D. The Agresso term written in lower case points to the Agresso as company.
ABW:	Agresso Business World, name of the complete product.
AGRESSO:	The AGRESSO term written in upper case points to the AGRESSO product itself.
AGRESSO POF:	AGRESSO PunchOut functionality
AGRESSO PO:	AGRESSO PunchOut
CORAS RMP:	CORAS risk management process

Table of contents

ABBREVIATIONS	116
TABLE OF CONTENTS	117
LIST OF TABLES	118
LIST OF FIGURES	119
EXECUTIVE SUMMARY	120
CHAPTER 1 INTRODUCTION.....	122
1.1 OBJECTIVES OF THE ANALYSIS.....	122
1.2 TEAM AND PLAN FOR THE ANALYSIS	122
1.3 THE CORAS FRAMEWORK FOR MBRA.....	125
1.4 REPORT STRUCTURE	126
CHAPTER 2 CONTEXT IDENTIFICATION.....	127
2.1 DESCRIPTION OF THE TARGET OF ANALYSIS	127
2.1.1 <i>AGRESSO PunchOut in a network</i>	128
2.1.2 <i>The AGRESSO PO process</i>	129
2.2 IDENTIFICATION AND VALUATION OF ASSETS	130
2.2.1 <i>Assets</i>	130
2.3 RISK EVALUATION CRITERIA.....	133
CHAPTER 3 RISK IDENTIFICATION.....	135
3.1 IDENTIFICATION OF THREATS AND UNWANTED INCIDENTS	135
3.1.1 <i>Exploitation of available information scenarios</i>	135
3.1.2 <i>Unavailable or slow service scenarios</i>	138
3.1.3 <i>Pipeline and configuration error</i>	143
3.1.4 <i>Manipulation of PostBack message</i>	146
3.1.5 <i>Mapping error</i>	148
CHAPTER 4 RISK ESTIMATION.....	149
4.1 CONSEQUENCE AND FREQUENCY ESTIMATION.....	149
CHAPTER 5 RISK EVALUATION.....	151
CHAPTER 6 RISK TREATMENT	153
6.1 RISK TREATMENT TABLE	153
6.2 TREATMENT RISK 11	155
CHAPTER 7 CONCLUSION	156
BIBLIOGRAPHY	158
DEFINITIONS	159
HAZOP QUESTIONS	160
HAZOP GUIDEWARDS.....	162
ANALYSIS TARGET.....	163

List of Tables

TABLE D 1 SUGGESTED TREATMENT.....	120
TABLE D 2 ANALYSIS ROLES TABLE.....	123
TABLE D 3 ANALYSIS PLAN TABLE	123
TABLE D 4 TARGET OF ANALYSIS TABLE.....	127
TABLE D 5 ASSET TABLE	131
TABLE D 6 VALUE DEFINITION TABLE.....	133
TABLE D 7 RISK MATRIX	134
TABLE D 8 CONSEQUENCE AND FREQUENCY TABLE	149
TABLE D 9 RISK EVALUATION TABLE.....	151
TABLE D 10 RISK MATRIX INCLUDED THE EVALUATED RISKS	152
TABLE D 11 RISK TREATMENT TABLE	153

List of Figures

FIGURE D 1 EXAMPLE USE OF CORAS'S GRAPHICAL LANGUAGE	125
FIGURE D 2 SIMPLIFIED AGRESSO NETWORK	128
FIGURE D 3 OVERVIEW AGRESSO PUNCHOUT FUNCTIONALITY	129
FIGURE D 4 OVERVIEW AGRESSO PUNCHOUT	130
FIGURE D 5 ASSETS	132
FIGURE D 6 R11	136
FIGURE D 7 R15	137
FIGURE D 8 R2 AND R3	140
FIGURE D 9 R5	141
FIGURE D 10 R6 AND R7	142
FIGURE D 11 R8	142
FIGURE D 12 R12	143
FIGURE D 13 R4, R10 AND R13	146
FIGURE D 14 R17	147
FIGURE D 15 R16	148
FIGURE D 16 TREATMENT RISK 11	155

Executive summary

This report documents the results from the security analysis conducted of the AGRESSO POF. The goal with the analysis was to improve the security in the functionality. To complete the security analysis the CORAS model-based risk assessment framework were used and the steps and suggested activities of the CORAS RMP were followed.

The viewpoint for the analysis was the Agresso organisation. There were identified values in the AGRESSO POF that were of relevance for Agresso. These assets guided the rest of the analysis. The three main assets were:

- Agresso's reputation
- Information
- Usability

The aim of the risk identification was to find potential losses in the assets. The threats and unwanted incidents were identified by performing a HazOp analysis. During the risk identification process there were discovered totally 17 potential risks. To evaluate what risks to treat the risks were added consequence and frequency values. The risks were prioritised from their risk values. It was recommended treatment to the risks of high value.

Recommended treatment to risks:

Table D 1 Suggested treatment

Risk ID	Threat scenario	Treatment	Vulnerability	Effect



In addition to the risks of high value there was also suggested treatment to the risks of medium value. These are presented in Table 1.

There were decided to review the analysis with a different viewpoint. The new viewpoint would not focus on the Agresso organisation, but have more technical view. The asset values will be more directed to the AGRESSO POF. The aim is to find risks that are directly attached to the AGRESSO POF.

Chapter 1

Introduction

Security threats are a subject that worries several enterprises. The threats on distributed systems increase. By using standards for risk management and carry out risk analysis, organisations can improve the quality in their systems and avoid occurrence of potential risks. SINTEF has developed a model-based framework, CORAS, to identify and remedy security risks.

Traditionally organizations system documentation focuses on the systems behaviour or functionality. However, it is equally important to document undesirable behaviour; what happens when things goes wrong? This report documents the threats and risks identified during the security analysis performed on the AGRESSO POF. It presents the objectives, the analysis team and plan, and an introduction to the CORAS MBRA (model-based risk assessment).

1.1 Objectives of the analysis

The analysis objective was to identify and analyse security risks related to the AGRESSO POF. The aim of CORAS is that it should be effective and easy to understand for all parts in an analysis involved and it should document threats and risks to the system that can cause undesirable behaviour. In order to evaluate the process there were collected feedback from the analysis participants. These evaluations would help the further research and improvement of CORAS.

This analysis was the first security analysis field trial accomplished in Agresso. The Agresso objective was to find advantages of using similar methods in future projects. If the Agresso participants find the method useful there is a wish to start using a simplified method in other similar projects.

1.2 Team and plan for the analysis

The analysis was carried out in the period January 2006 to March 2006 and managed by Jenny B. Hougen under supervision from SINTEF. In order to

accomplish the analysis an analysis team were compounded. The team consisted of people with different knowledge about the system. Table 2 gives an overview of the people involved in the security analysis and their role and background.

Table D 2 Analysis roles table

Name	Role
Jenny Beate Hougen	Analysis leader
Tor Gaute Indstøy	Security expert, system designer, analysis secretary
Erik Inge Marcussen	Developer, AGRESSO framework expert
Randi Bjørnbeth	System designer
Truls Tveøy	System designer, developer
Helge T. Blindheim	Customer view

To carry out the analysis and get a correct understanding of the target, it requires good communication between the analysis team. Structural meetings were accomplished. The required tasks and dates for the meetings are displayed the Table 3.

Table D 3 Analysis Plan Table

Task ID	Description	Performed date	Participants
Context identification 1	UML models with descriptions from the documentation given about the PunchOut requisition were prepared. The models were reviewed to get a clear understanding of the target. The second task for the meeting was to decide the rest of the team to participate in the analysis.	10.01.2006	Tor Gaute Indstøy, Erik Inge Marcussen, Jenny Hougen
Context identification 2	The team were introduced and a short introduction to CORAS was applied. The participants went through the target models created by the analyst leader. The activity terminated when the team were satisfied with the target description.	24.01.2006	Randi Bjørnbeth, Tor Gaute Indstøy, Helge T. Blindheim, Erik Inge Marcussen, Truls Tveøy, Jenny Hougen
Risk identification 1	This meeting started with an approval from the last	01.02.2006	Randi Bjørnbeth, Tor Gaute Indstøy,

Task ID	Description	Performed date	Participants
	meeting. The participants were divided into two teams for accomplish a structured brainstorming. PunchOut documentation and checklist was handed out. Based on the hand outs the team should fill out the risk table.		Helge T. Blindheim, Erik Inge Marcussen, Truls Tveøy, Jenny Hougen
Risk identification 2	Continued the structured brainstorming. The activity terminated when the team could not find more risks. The participants went through each unwanted incident scenario found.	08.02.2006	Randi Bjørnbeth, Tor Gaute Indstøy, Helge T. Blindheim, Erik Inge Marcussen, Truls Tveøy, Jenny Hougen
Risk estimation and evaluation	The analyst leader had created CORAS unwanted incident diagrams. These were handed out. Consequence and frequency values were decided. The goal of the meeting was to determine consequence and frequency values to the unwanted incidents.	14.03.2006	Randi Bjørnbeth, Tor Gaute Indstøy, Helge T. Blindheim, Truls Tveøy, Jenny Hougen
Risk estimation and evaluation	Continued applying the consequence and frequency to the unwanted incidents.	20.03.2006	Randi Bjørnbeth, Tor Gaute Indstøy, Helge T. Blindheim, Truls Tveøy, Jenny Hougen
Risk treatment	Risk treatment approval and project closing.	21.04.2006	Jenny Hougen, Randi Bjørnbeth, Tor Gaute Indstøy Erik Inge Marcussen, Truls Tveøy, Jan Åge Berg, Ida Camilla Egeland.

1.3 The CORAS framework for MBRA

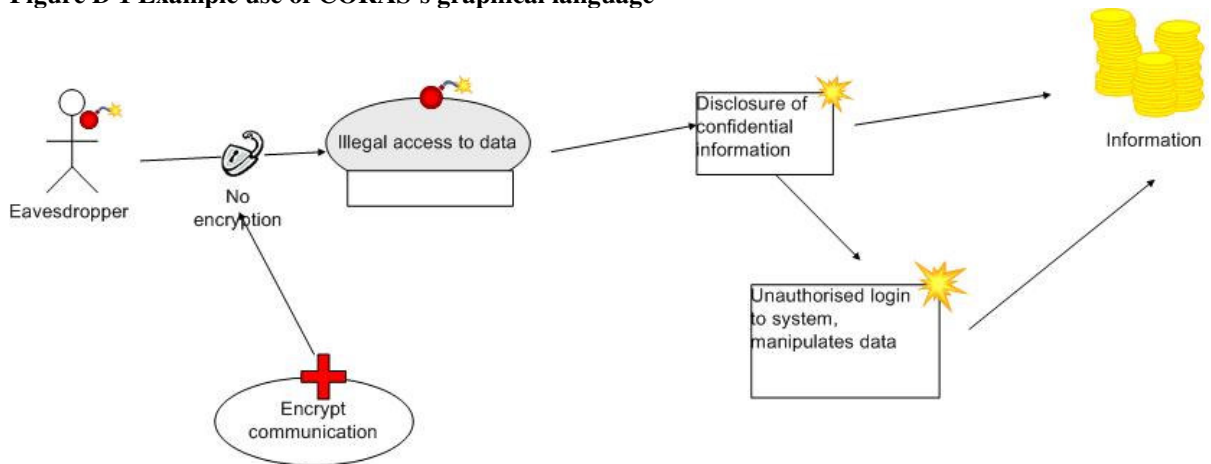
CORAS is a method for doing risk assessment of security critical systems. CORAS's purpose is to help integrate security into system development. One of the main objectives of CORAS is to develop a practical framework to support and simplify risk management. The framework includes the result from use of experience library from previous projects, the methodology for doing risk assessment and terminology used in the projects. [2]

The aim of a risk analysis is to suggest actions that will control the unwanted incidents (avoid or reduce the consequence of the unwanted incidents).

“A threat is by definition dangerous and therefore important. When it comes to human beings, many threats are reflected instinctively. Any snake, even the non lethal ones, scares most of us. This is because through evolution we have indirectly experienced many dangerous situations with snakes involved. When it comes to information systems we lack this experience. While a snake can scare us without carrying a note saying: “if you are a human being, I might be a threat to you”, the threats connected to information systems must be documented in a clear and understandable way for us to see them. Documenting threats in a clear and understandable way is what threat modelling is all about “. [1]

The CORAS framework for model-based risk analysis (MBRA) contains a graphical language for document threats and unwanted incidents. An example of how the CORAS UML profile can be used is given in Figure D 1.

Figure D 1 Example use of CORAS's graphical language



Unwanted incidents diagrams consist of threats and unwanted incidents. The threat scenario may be caused by a weakness, vulnerability, in the system that the threat agent can exploit. The threat agent (e.g. eavesdropper or malicious person) present the active part of the threat and the threat scenario is behaviour of the threat agent. A threat scenario may lead to an unwanted incident. The threats and the unwanted

incidents are related to the assets they threat. In this case the threat agent is an eavesdropper that could get illegal access to data by listening to the network. This arises because of the lack of encryption in the network. This threat could cause an unwanted incident of disclosure of confidential information. The risk could easily be treated by encrypting the communication.

1.4 Report structure

This section presents the report structure. It is meant as a help to the reader and summarises the main points from each chapter.

CHAPTER 1: Establish the purpose and goal for the analysis and contains information about the participants and meetings completed. The chapter introduces the reader to the CORAS framework for MBRA.

CHAPTER 2: Documents and describes the analysis context which includes a description of the analysis target, the asset related to the target and risk evaluation criteria used later in the report.

CHAPTER 3: Documents the result of the risk identification process. It Categorise the unwanted incidents scenarios into appropriate sections.

CHAPTER 4: Documents the estimated unwanted incidents.

CHAPTER 5: Documents the evaluation of the risks and gives the result of which risk that should be treated.

CHAPTER 6: Suggest a solution to the risk decided to treat.

CHAPTER 7: Gives a short conclusion with suggested further work.

Chapter 2

Context identification

The aim of this process was to identify the context of the analysis; what was the purpose of this analysis? What do we want to protect? Which risk level are we willing to accept? This includes describing the environment, the target, identify assets and specify risk acceptance criteria. There were provided a correct and complete description of the AGRESSO POF and its environment. The description is presented in the form of pictures, models and text.

2.1 Description of the target of analysis

The target of the analysis is the PunchOut process in the ABW (Agresso business world) system. Agresso's goal is to create a more flexible PunchOut solution. The new design should give room to accommodate customers need. PunchOut is the process of sending the requisition from AGRESSO Self Service to the marketplace and the marketplace replying on these messages. The goal is to improve the security in the functionality. Table D 4 gives a short target description including the analysis client, target functionalities and analysis quality aspects.

Table D 4 Target of Analysis table

Category	Value
Target	The AGRESSO POF, web application. The process when transferring (punch-out) messages between an AGRESSO Self Service and a marketplace and reply on the message.
Client	Agresso R&D
Service/Function	PunchOut Go shopping (the process of enter the marketplace to shop) PostBack (the process when marketplace post back the message to AGRESSO) Retrieve shopping (the user loads the message into the browser) Delete purchase (the user deletes a purchase) Approve purchase (the user sends the requisition to a approver)
Quality aspects	Client authentication, server authentication, confidentiality,

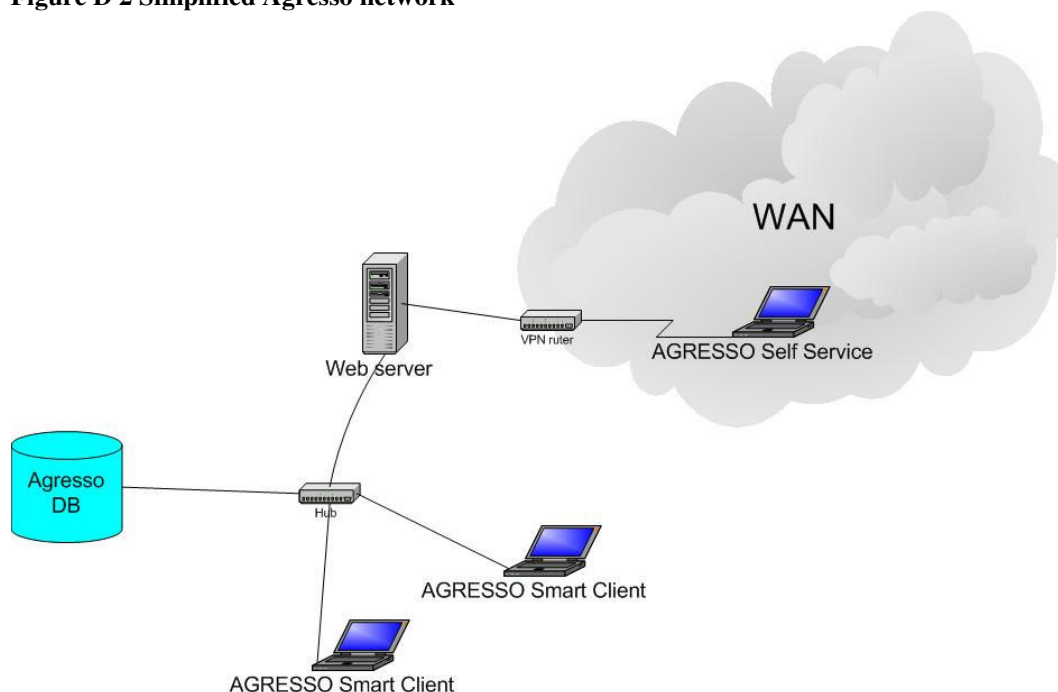
Category	Value
	integrity

In the following there will be described the role of the AGRASSO POF in a typical Agresso network, who has legal access to the functionality, communication between the components in the functionality and description of the PunchOut processes.

2.1.1 AGRASSO PunchOut in a network

ABW consist of a windows application named AGRASSO Smart Client and a web application named AGRASSO Self Service as illustrated in Figure D 2 The AGRASSO POF could only be accessed from the AGRASSO Self Service application. If an Agresso user wishes to use AGRASSO through internet the user has to connect the Self Service through a VPN (virtual private network) connection.

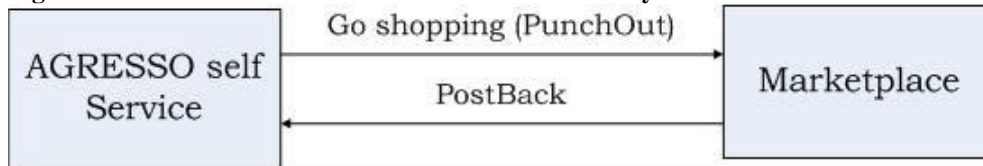
Figure D 2 Simplified Agresso network



2.1.2 The AGRESSO PO process

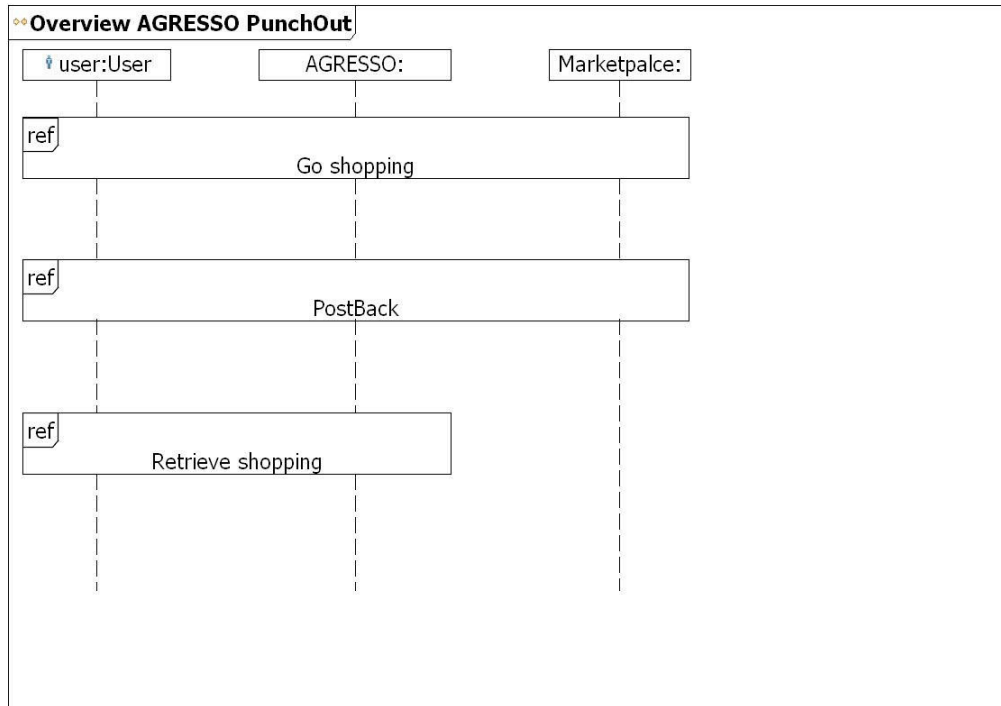
PunchOut is the process of transferring message between AGRESSO and the marketplace as illustrated in Figure D 3. The user pushes “go shopping” to enter the marketplace. When the user is finished the requisitions is posted back to AGRESSO.

Figure D 3 Overview AGRESSO PunchOut functionality



The AGRESSO PO was divided into three processes:

- *Go shopping*: The process of enter the marketplace to shop. User push “Go shopping” button.
- *PostBack*: The process when marketplace posts back the message to AGRESSO.
- *Retrieve shopping*: The user loads the message into AGRESSO (requisition site) from the message inbox.

Figure D 4 Overview AGRESSO PunchOut

A more detailed description of the three processes is presented in the following sections.

2.2 Identification and valuation of assets

This section gives a description of the assets relevant to the AGRESSO POF. The process included finding what is of value in the target of analysis from an enterprise view, the Agresso Company, viewpoint. The Agresso assets that are related the AGRESSO POF.

2.2.1 Assets

Assets are something with value that is vulnerable for Agresso if it loses value (e.g. the asset Agresso clients, if Agresso loses clients then Agresso will lose income thus Agresso client is something valuable for Agresso)

The assets relevant for the AGRESSO POF are given in Table D 5. It was identified three main assets to use during the risk identification:

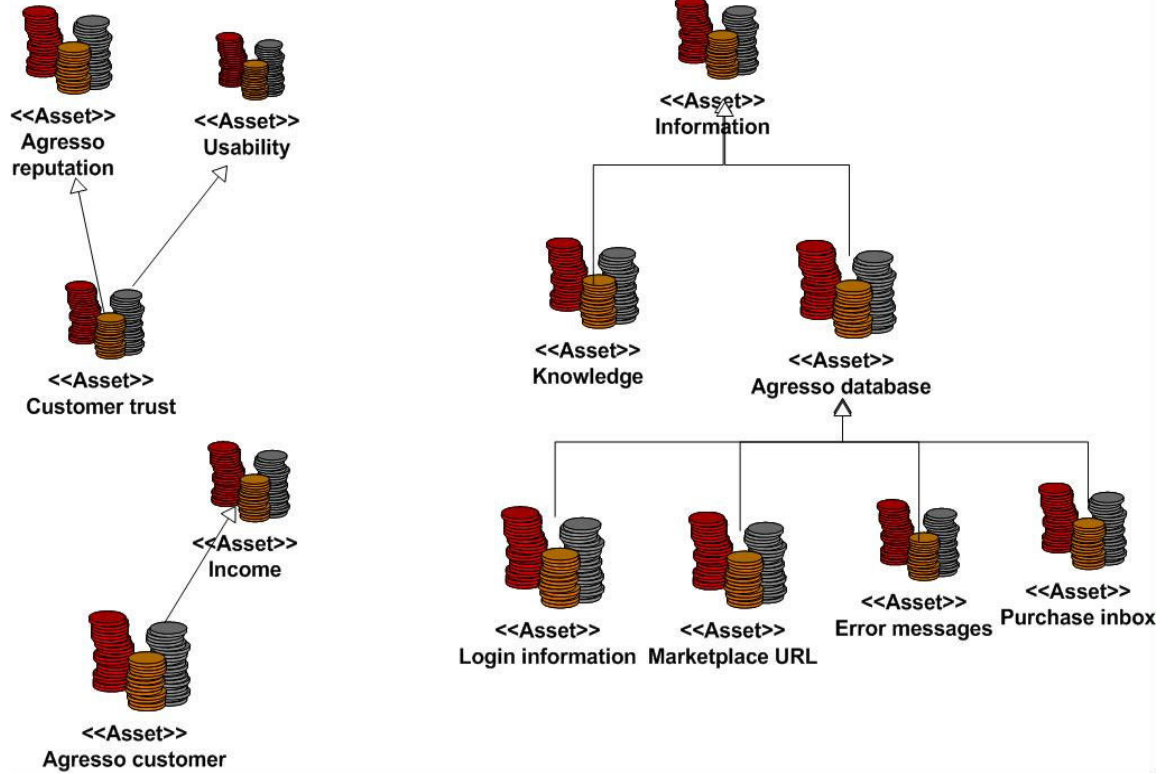
- Agresso Reputation
- Information
- Usability

Table D 5 Asset Table

Asset ID	Description	Category
A1	Agresso's reputation in the market. A loss in reputation will affect customers trust and Agresso may lose customers	Agresso Reputation
A2	Misuse of information may cause damage on customers' data and confidential information. It would put Agresso in a bad view and could affect trust and loss of customers.	Information
A3	The customer expects that AGRESSO would work properly.	Usability

In additional to the three main asset there exist asset related to these.
 This model gives an overview of possible assets in AGRESSO POF and the relation between them.

Figure D 5 Assets



2.3 Risk evaluation criteria

In order to decide the level of risk to the identified threats and unwanted incidents there were defined risk evaluation criteria, given in Table D 6. It defines the frequency, consequence and risk values. The frequency, consequence and risk values are added to the risk matrix.

The risk value is decided by the incidents consequence and frequency values, and is used to decide what loss in asset value Agresso can tolerate.

Table D 6 Value Definition Table

Type	Domain	Allowed values	Description
Frequency	occurrence/time	very rare, rare, usual	Very rare: 1:year Rare: 1/4:year Usual: 1:week
Consequence	NOK	low, medium, high	Low: 100 000, No noticeable effect Medium: 1 000 000, Loss of potential customers High: 10 000 000, National effect
Risk value		low, medium, high	Low: accept Medium: Monitor High: Treat

The risk matrix in Table D 7 consists of the frequency, consequence and risk values defined in the value of definition table.

Table D 7 Risk Matrix

	Frequency			
Consequence		Very rare: <i>1 : Year</i>	Rare: <i>1/4 : Year</i>	Usual: <i>1 : Week</i>
	Low: <i>100 000 NOK, no significant effect</i>	Low	Low	Low
	Medium: <i>1 000 000 NOK, loss of potential customers</i>	Low	Medium	Medium
	High: <i>10 000 000 NOK, national effect</i>	High	High	High

Chapter 3

Risk identification

This section documents the risk found during the risk identification process. The goal of this process is to identify threats to assets. During the process there were used a known risk analysis method Hazard and Operability Analysis (HazOp). Two risk identification meetings were accomplished, organised as structured brainstorming. In the brainstorming session the system documentation of the three main processes in the AGRESSO PO were handed as input together with guidewords and questions (see end of this report).

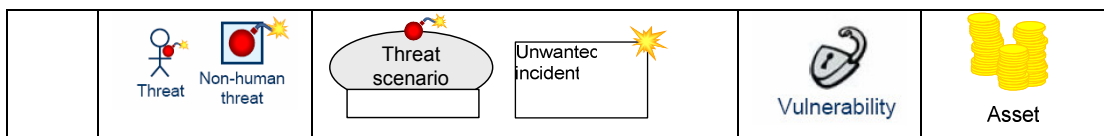
3.1 Identification of threats and unwanted incidents

During the brainstorming session the analysis team identified possible threats and unwanted incidents. The incidents were given frequency values assigned by the analysis team (presented in Chapter 4).

The incidents are logical structured. Similar risks are put together and described. The identified threats and unwanted incidents are categorised and described in a HazOp table and a more detailed description is given with CORAS own graphical language (introduced in section 1.3). The HazOp table describes the threat agent, unwanted incidents and vulnerabilities to each possible risk.

3.1.1 Exploitation of available information scenarios

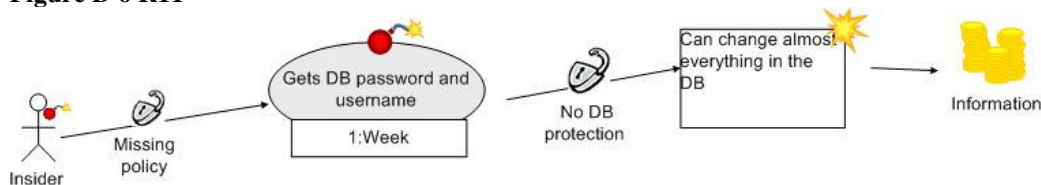
In organisations much information circulates. Some information is confidential and need protection. A malicious person can exploit the available information. This section describes the exploitation of available information unwanted incidents scenarios identified in the AGRESSO POF.



Risk ID	Who/what caused the incident?	How? What is the incident?	What makes this possible?	What will harm it?
R11	Human threat, insider	The insider gets the DB password and username. Can change almost everything in the database.	Missing enterprise policy. No DB protection.	Information (Agresso DB)
R15	Human threat, eavesdropper, competitor	An eavesdropper listens to the traffic between AGRESSO and the MP and gets valuable information. Access to MP login information, get access to contract data. Media publicity about expensive contracts that could harm Agresso. Exposing of contracts. Information that could harm the reputation. Access to DB password, overwrites/destroys data Intercept confidential information. Could cause overview of shopping patterns and a new supplier can adjust the supply.	Missing information protection. No encryption	Information, reputation

R11 scenario: The R11 scenario is given in Figure 6. The scenario shows what could happen if Agresso has a weak organisation policy. Most of the attacks in an organisation are caused by an insider. If a malicious insider gets the DB login information he could do a lot of damage on the system. Weak organisation policy of who should have the DB login information would increase the chance of information getting into wrong hands.

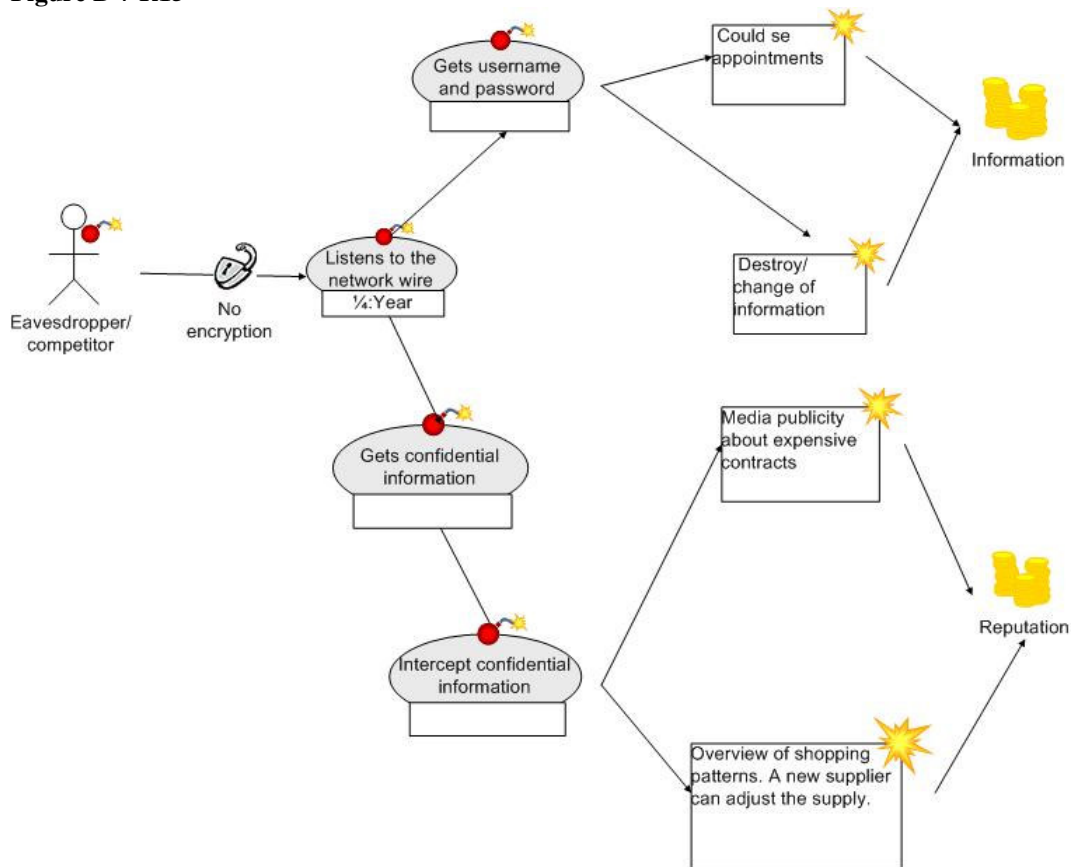
Figure D 6 R11



R15 scenario: R 15 illustrates an eavesdropper/competitor listens to the communication between the MP and Agresso. Packets are transmitted from the Marketplace to AGRESSO during a shopping session. If the communication is not secured packets are vulnerable for attacks. Scenarios that may occur:



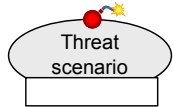



- Eavesdroppers can listen to the network and read confidential information.
- Agresso competitors could exploit this vulnerability and create media publicity about expensive contracts etc.
- A supplier can get overview of the shopping patterns and adjust the supply to gain profit.
- An eavesdropper can also change the information in the packets transmitted between AGRESSO and the Marketplace.

Figure D 7 R15



3.1.2 Unavailable or slow service scenarios

The system usability is important for a user. A slow system or not accessible system is not a good system. A variety of attacks can result in the loss of or reduction in availability. This section describes identified incident that could cause unavailable or slow PunchOut service.

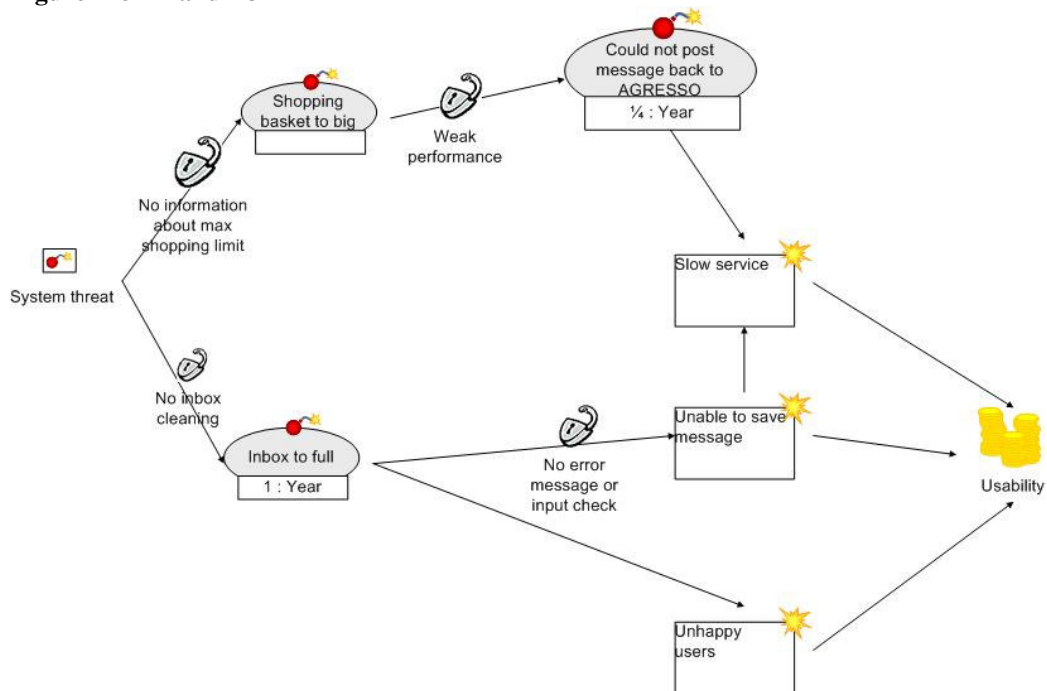
	 Threat  Non-human threat	 Threat scenario  Unwanted incident	 Vulnerability	 Asset
Risk ID	Who/what caused the incident?	How? What is the incident?	What makes this possible?	What will harm it?
R2	System threat	Shopping basket is too big. Could not post back message to AGRESSO. Slow service.	Weak performance. No information to user about maximum shopping limit.	Usability
R3	System threat	Inbox to full. Information will not be saved/ Inbox becomes too large. The searching time gets to long. Results in slow service that will affect the usability. Too many purchases. Top Gen will not be able to load purchases when the user pushes “retrieve shopping”. The user will not be able to delete.	Lack of error message. No inbox cleaning. No limit on how many purchases the user can load.	Usability
R12	Human threat, Hacker (competitor, partner, insider)	Large messages are posted to the server. Causes a DoS attack. The service gets unavailable or slow. Authorized users get no work done.	Not protected against DoS attack.	Usability
R5	System threat, performance	Too many users using PunchOut. The system shuts down. The service becomes unavailable.	Poor infrastructure/ bad performance	Usability

R6	Attacker	Dos attack. The system is shutting down; the users lose work and have to do the work over again.	Missing error handling and logging.	Usability
R7	System threat	The system is shutting down, the users lose work and have to do the work over again: Timeout (the session times out) Web server reboots.	Missing error handling and logging.	Usability
R8	Customers infrastructure	PunchOut can not be enabled. Users are not able to shop.	Missing support in customers' infrastructure. Users could not access internet. Customer requires strong security.	Usability

R2 and R3 scenario: R2 and R3 shows two incidents that would cause in unavailable or slow service. The PunchOut functionality has lacks that may affect the usability. The lack of shopping limit in the PunchOut functionality makes it possible for the user to send large and unwieldy packets to AGRASSO. This may result in that the PunchOut service will either reject it or the service is getting slow.

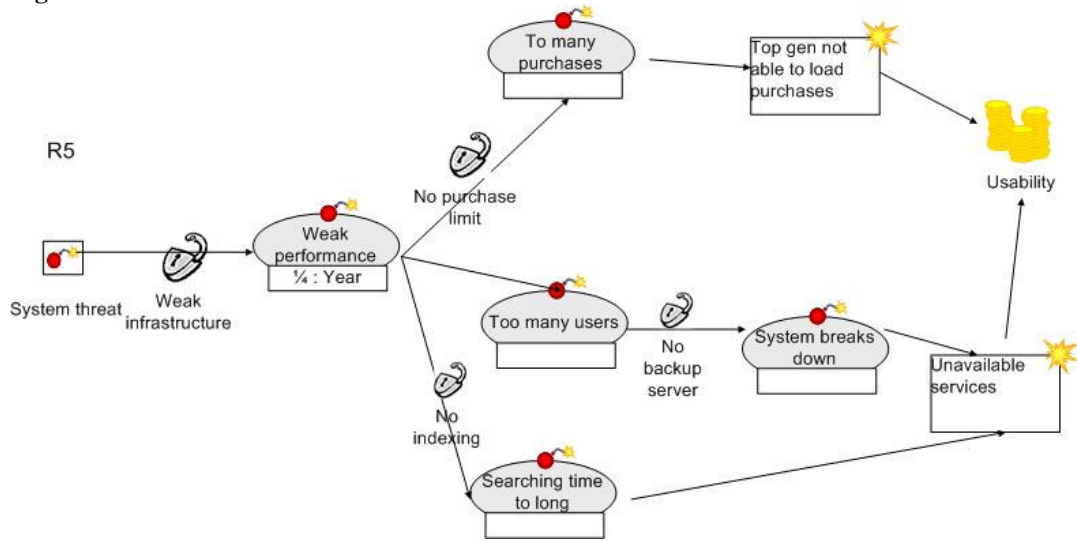
Another scenario of slow service is if the inbox is full or large. This could cause slow and unavailable service. If the user wishes to upload purchases the time of getting the purchases could take a while. The lack of inbox indexing could cause in long searching time.

Figure D 8 R2 and R3



R5 scenario: The R5 scenario demonstrates what could happen if the Agresso customer have weak infrastructure. The infrastructure may not be able to handle several purchases. If shopping basket message is too big or several users post back messages to the system at the same time, the service could be slow. This will cause in a slow service and TopGen will not be able to load purchases. There could also be too many users using PunchOut that could in worst case cause a system break down.

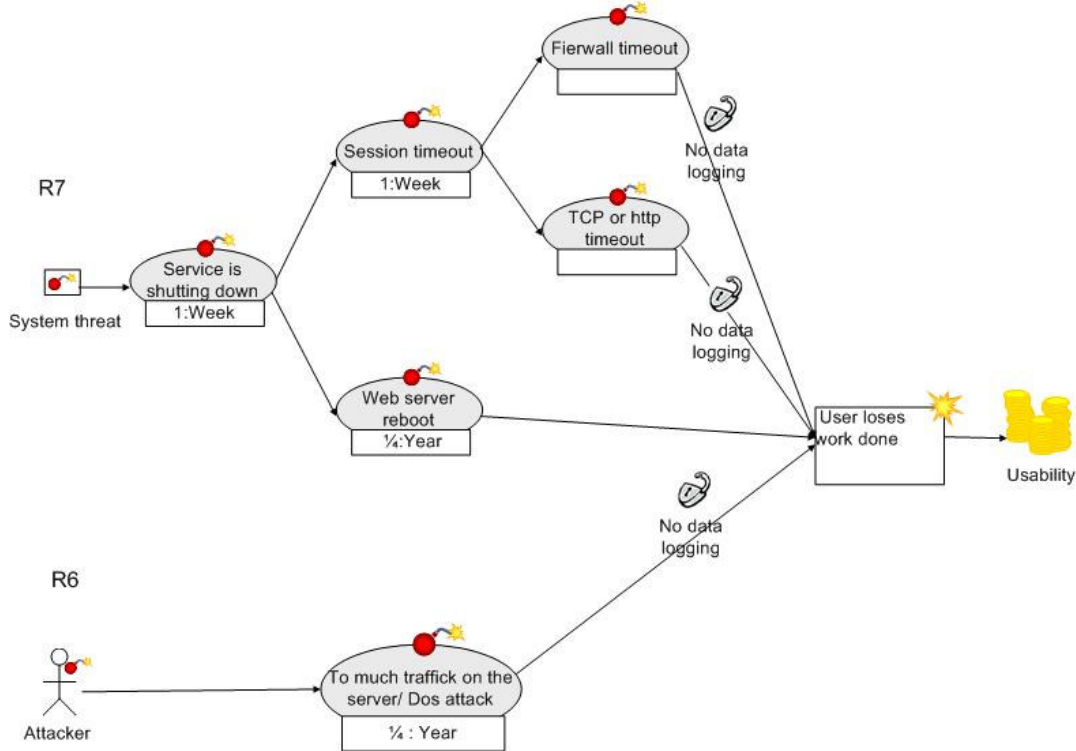
Figure D 9 R5



R6 and R7 scenario: Unavailable or slow service could have influence at the users work. If the user shops in a Marketplace and post back the shopping basket to AGRESSO while the service becomes unavailable the work will be lost. A session timeout or a web server reboot could cause this action.

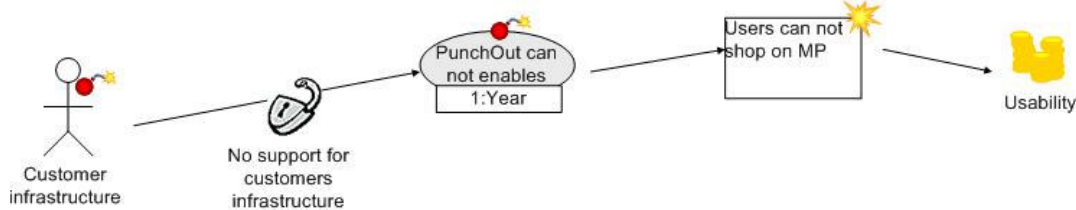
Another scenario is a Denial of service (DoS). An attacker could send large and heavy packets to the server. A possible DoS attack is the known SYN attack.

Figure D 10 R6 and R7



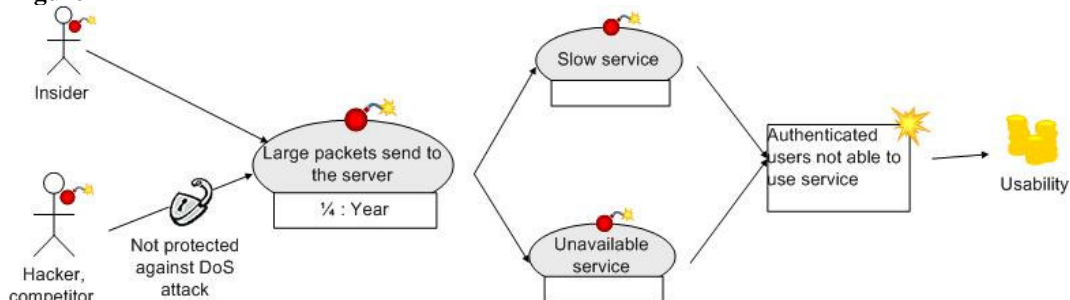
R8 scenario: In addition to R5 the Agresso customer infrastructure may not support PunchOut at all. It could be that the customer has strict security that does not allow PunchOut to enables. It will result in unavailable PunchOut service.

Figure D 11 R8





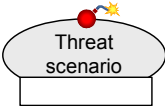
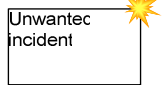


R12 scenario: As illustrated inFigure14, an insider or hacker could also affect the usability by sending large and many packets to the service and cause a DoS attack. This causes a slow or a not accessible system at all. Then authenticated users are not able to use the service.

Figure D 12 R12



3.1.3 Pipeline and configuration error

This section describes the incidents identified pursuant to the pipeline and configuration file errors in the AGRASSO POF.

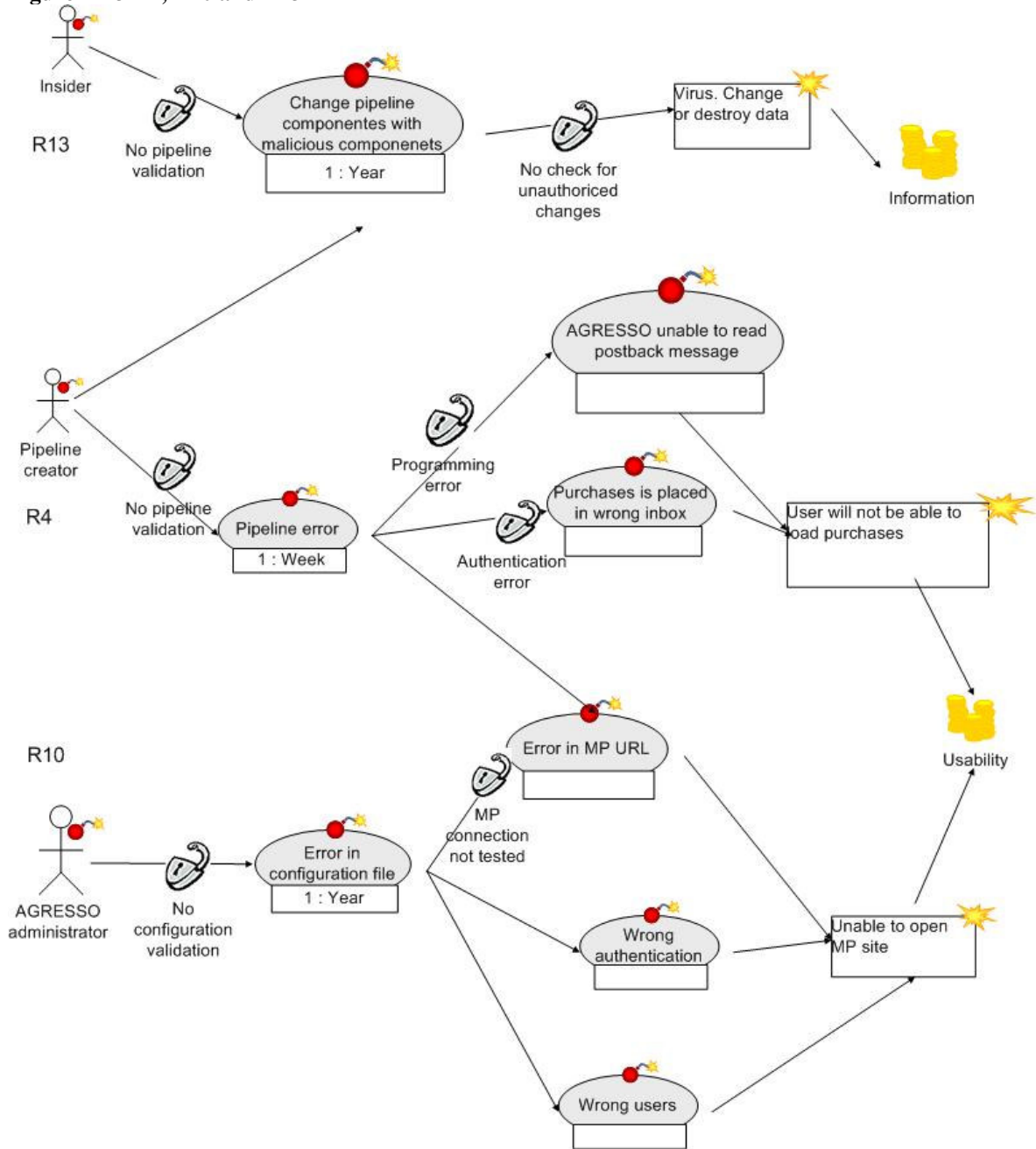
	  Threat Non-human threat	  Threat scenario Unwanted incident	 Vulnerability	 Asset
Risk ID	Who/what caused the incident?	How? What is the incident?	What makes this possible?	What will harm it?
R4	System threat, pipeline creator	Pipeline error. The pipeline creator writes incorrect and bad code. Error in MP URL. The user gets redirected to another MP or no side. AGRASSO could not read the PostBack message. Wrong format in the PostBack message. MP sends a PostBack message to AGRASSO. The message is placed in the wrong inbox.	No validation of pipeline components, unauthorized allowed changing components. programming error Authentication error	Usability
R10	Human threat, AGRASSO administrator	The administrator gives wrong information in the configuration file Error in MP URL, the user access wrong MP or no MP at all. Error in user information.	Error in the configuration, master file. The connection is not tested.	Usability

		The users can not access MP Error in authentication information.		
R13	Human threat, insider	An insider changes the replaces the pipeline components with own made components. The components could harm the system.	There exists no validation/approval of pipeline components. No integrity check. Missing input check in the AGRESSO framework.	Information

R4, R10 and R13 scenario: These scenarios present the incidents of human threats to the AGRESSO POF. Aggresso adjusts that other than the developers can create their own pipeline components in the POF. Insiders and pipeline creators could misuse their authority to change the pipeline components with malicious code e.g. virus (R13). R4 illustrates the lack of pipeline validation. Since there does not exist any form of pipeline validation, pipeline creators could create errors in the pipeline components.







The AGRESSO administrator configures the PO. The administrator decides who should have access and what Marketplace to connect. If the administrator adds wrong configuration settings, the PO will not work properly (R10).

Figure D 13 R4, R10 and R13



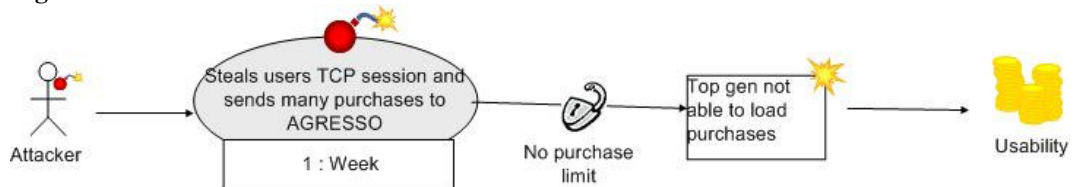
3.1.4 Manipulation of PostBack message

The Agresso user post back messages from the Marketplace to AGRESSO. This operation is vulnerable since AGRESSO is connected to the Marketplace internet page. This section involves the incidents identified related to events of when a user posting back a message from the Marketplace to AGRESSO.

	 Threat	 Non-human threat	 Threat scenario	 Unwanted incident	 Vulnerability	 Asset
Risk ID	Who/what caused the incident?	How? What is the incident?	What makes this possible?	What will harm it?		
R17	Human threat, attacker	An attacker steals a users TCP session and uses the session to send several purchases to AGRESSO. Top Gen will not be able to load purchases because it is too many. The user could not delete the purchases because Top Gen will not load them.	No purchase limit.	Usability		


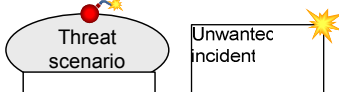


R17 scenario: The attacker could use the session to send several or large purchases to AGRESSO. Since there is a lack of purchase limit the attacker (or an Agresso user) could send a large packet to AGRESSO. This could cause in unavailable PunchOut service.

Figure D 14 R17



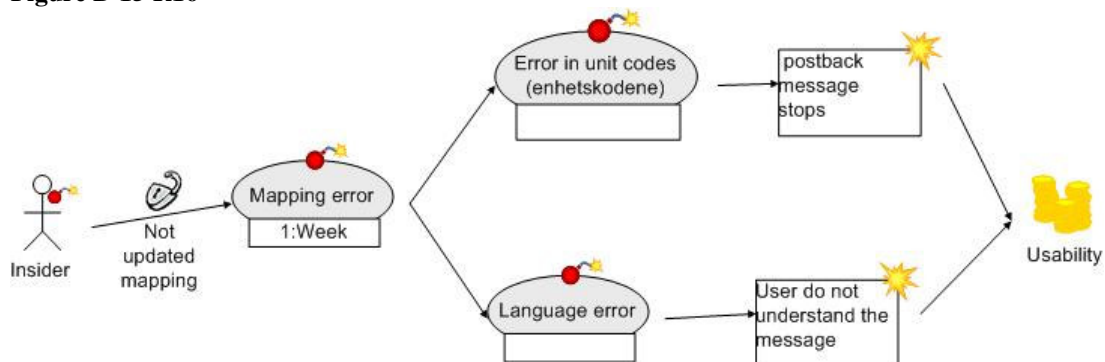
3.1.5 Mapping error

When using AGRESSO there occur several mappings. It could be language mapping, (translation of a language) or unit code mapping (purchase mapping). This scenario describes incidents when mapping error occurs.

				
Risk ID	Who/what caused the incident?	How? What is the incident?	What makes this possible?	What will harm it?
R16	Human threat, insider	The AGRESSO mappings are not updated. Error in unit codes or language.	Missing/not updated mapping between unit codes	Usability

R16 scenario: R26 shows the incidents of mapping error in PunchOut functionality. There are two mapping scenarios could occur. If the purchases the Agresso post back to AGRESSO has wrong unit codes, it will be rejected and not be able to load the purchases into AGRESSO. The other scenario could be if there exist translation errors. Then the user will probably misunderstand the messages because they are written in another language than the user expects it to be written in.

Figure D 15 R16



Chapter 4

Risk estimation

The identified risks were given consequence and frequency values. This chapter gives the result of these estimated values.

There was a lack of logs and documentation that could help decide the frequency values, thus the values are based on the teams experience and logic. The values considered all the AGRESSO applications installed in Norway.

4.1 Consequence and frequency estimation

Table D 8 table adds consequence and frequency values to the unwanted incidents found in the risk identification process.

Table D 8 Consequence and Frequency Table

Risk ID	Asset ID	Incident	Consequence Value	Frequency Value
R1	A2	Malicious person hacking AGRESSO	high	Rare
R2	A3	Shopping basket to big	low	Rare
R3	A3	Full inbox	low	Very rare
R4	A3	Pipeline error	low	Usual
R5	A3	Unavailable service	low	Rare
R6	A3	High traffic on the server, user loses work.	low	Rare
R7	A3	Service is shutting down	low	Usual
R8	A3	User not able to shop on MP	low	very rare
R9	A2	Manipulation of post back message	medium	Rare
R10	A3	Error in configuration file	low	very rare
R11	A2	Unauthorised change in the database	medium	Usual

Risk ID	Asset ID	Incident	Consequence Value	Frequency Value
R12	A3	Authenticated users not able to use service	low	Rare
R13	A2	Insider change pipeline components	medium	very rare
R14	A2	Malicious person get valuable information about AGRASSO	high	Usual
R15	A1	Eavesdropper listens to the network and get confidential information	low	Rare
R16	A3	Mapping error	low	Usual
R17	A3	Top Gen not able to load purchase	medium	Usual

Chapter 5

Risk evaluation

In order to find risks to treat there were assigned risk values to each risk. The risk values are determined from the consequence and frequency values given in Table D 8.

Based on the result from the consequence and frequency estimation each risk was assigned a risk value. From the value of definition table the risk level were prioritised.

Table D 9 present the risks added to the risk matrix.

Table D 9 Risk Evaluation Table

Risk ID	Risk Value	Risk Priority
R1	High	Treat
R2	Low	Accept
R3	Low	Accept
R4	Low	Accept
R5	Low	Accept
R6	Low	Accept
R7	Low	Accept
R8	Low	Accept
R9	Medium	Monitor
R10	Low	Accept
R11	Medium	Monitor
R12	Low	Accept
R13	Low	Accept
R14	High	Treat
R15	Low	Accept
R16	Low	Accept
R17	Medium	Monitor

Table 10 displays the risk added into the risk matrix. It indicates that R1 and R14 are high risk and should be treated.

Table D 10 Risk matrix included the evaluated risks

Consequence	Frequency			
		Very Rare <i>1 : Year</i>	Rare <i>¼ : Year</i>	Usual <i>1: Week</i>
Low: <i>100 000</i> <i>NOK, no</i> <i>significant</i> <i>effect</i>		R3,R10,R8	R2,R5,R6,R12,R15	R4,R7,R16
Medium: <i>1 000 000</i> <i>NOK, loss</i> <i>of potential</i> <i>customers</i>		R13	R9	R17,R11
High: <i>10 000 000</i> <i>NOK,</i> <i>national</i> <i>effect</i>			R1	R14

Chapter 6

Risk treatment

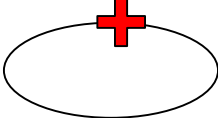


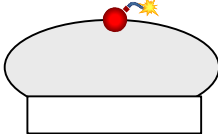
The main goal of the risk treatment is to reduce either consequence or frequency values of the risks. In a treatment diagram the treatment specified as a use case addressing the treatment to an unwanted incident.

There is suggested treatment to the risks of medium and high risk value as given in Table D 9 (Chapter 5). The first section describes the treatment in a treatment table. The following section describes each of the treatments with CORAS's specific graphical language.

6.1 Risk treatment table

The risk treatment table describes the treatment and the treatment effect of the risk decided to treat.

Table D 11 Risk treatment table

Risk ID	Treatment 	Vulnerability 	Effect 	Threat scenario 
R11	Apply strict access policy	Missing policy	Less people have access to DB information will reduce the likelihood of misuse of information.	The insider gets the DB password and username. Can change almost everything in the database.

R11	Configure the DB securely	No DB protection	Reduces the likelihood for possible attacks	The insider gets the DB password and username. Can change almost everything in the database.
------------	---------------------------	------------------	---	--

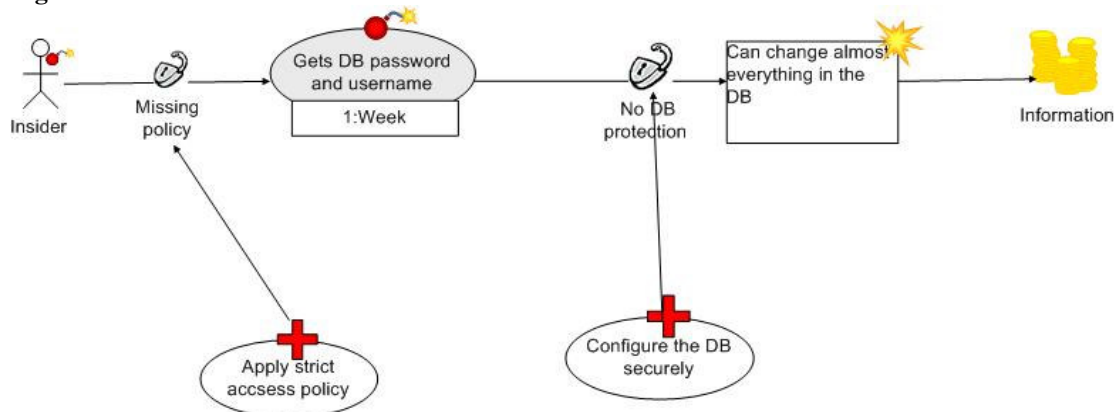
6.2 Treatment Risk 11

Treatment R11: The R11 identified two vulnerabilities missing organisation policy and lack of DB protection. A solution to the missing policy could be to apply strict access policy e.g. use known standards to apply good access policy to the organisation.

In order to protect the DB there are several actions that can be applied. In the following some are listed:

- Enforce integrity (e.g. in MS SQL entity integrity, domain integrity, referential integrity and user defined integrity)
- Avoid using the guest account
- Access control. Use windows authentication
- Database encryption
- Auditing the DB

Figure D 16 Treatment Risk 11



Chapter 7

Conclusion

The aim of the analysis was to find potential security issues in AGRESSO POF and thereby improve it. In order to find potential risks we had to decide the elements of value (assets). The viewpoint of the analysis was Agresso, thus the assets were determined from the Agresso organisations viewpoint. There were three main assets considered during the process:

- Agresso Reputation
- Information
- Usability

In the risk identification process the goal was to find potential risk that could cause a loss of these assets. There were accomplished a structured brainstorming to find the risks. In the brainstorming there were handed out checklist and question with intention to assist the analysis team in finding risks. The AGRESSO POF is divided into three parts, each examined in the brain storming process:

- Go shopping
- PostBack
- Retrieve shopping

When the risks were identified, each was estimated with consequence and frequency value. Since there did not exist any information (e.g. logs) of attacks etc. the team used their own experience and logic to estimate the risks.

Conducting to the Agressos' viewpoint two risks of high value was found:



It is difficult to give a good solution to any of these risks. They are both general and do not describe in detail how it could happen.

The AGRESSO POF itself is not a critical part of Agresso, thus with an Agresso viewpoint there will not be any high risks of interest for the AGRESSO POF.

To summarise this analysis could be more directed to the AGRESSO POF and not as much the Agresso organisation. Thus it is suggested to conduct an upgraded meeting. Suggestion for further work to improve the analysis result follows.

Further work

In order to upgrade the analysis the analysis will be reviewed. The aim is to find more threats related to the AGRESSO POF. In this case the viewpoint will be AGRESSO POF. As input to the process the result of this analysis will be given.

The process will include extra meeting with new assets and viewpoint. It could be performed an actual test in the test environment. Recommended points of interest in the new process are:

- Performance
- Authentication handling
- Session handling
- Error handling
- Information flow.

This process will be a more practical. Tools like fiddler¹¹ would be used.

¹¹ <http://www.fiddlertool.com>

Bibliography

- [1] “The CORAS framework, the CORAS UML profile for security assessment, and the CORAS library of reusable elements”
<http://coras.sourceforge.net/documents/SINTEF-deseca-report.pdf>, 19-04-2006
- [2] Mass Soldal Lund, Ida Hogganvik, Fredrik Seehusen, Ketil Stølen: “CORAS, Risk Assessment of Security Critical Systems”, version 1.0 (03.037 WP3 Act 3.6 D3.7)
- [3] AS/NZS 4360 (1999): Australian Standard: Risk Management. Standards Australia, 1999.

Definitions

Frequency:	A measure of the rate of occurrence of an event expressed as the number of occurrences of an event in a given time. (Likelihood and Probability). The frequency of a loss in Asset. [2]
Consequence:	The outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event. [2]
Risk:	The chance of something happening that will have an impact upon objectives. It is measured in terms of consequence and frequency. A risk is an unwanted incident that has been assigned consequence and frequency values. The level of risk is decided by the consequence and frequency values. [2]
HazOp:	Hazard and operability study. It is a technique for identifying and analyzing the hazards and operational concerns of a system. [2]
Threat:	A potential cause of an unwanted event, which may result in harm to a system or organisation and its assets
Risk analysis:	Systematic process to understand the nature of and to deduce the level of risk [3].
Security analysis:	A special form of risk analysis focusing on security risks.

HazOp questions

Generelt:

Hvem kan såre oss? Hva er motivasjon og mål?

Hvor mye kunnskap har de om systemet?

Bruker feil:

Kan brukeren gjøre feil?

Hva skjer hvis brukeren gjør en feil?

Kan bruker slette noe han/hun ikke skal slette?

Systemfeil:

Gir systemet unødvendig mye informasjon? F.eks feilmeldinger.

Kan informasjonen utnyttes av en intranger?

Hvordan er systemets ytelse?

Hva skjer hvis det er stor pågang mot siden? Dos attack

Hvordan er feilhåndteringene?

Hvordan er logikken i systemet?

Hvordan er informasjons flyten? Er det unødvendig informasjons flyt?

Forsinkelse

Programeringsfeil

Hvordan håndteres autentiseringen?

Krav fra kunden:

Påvirker PunchOut kundenes krav?

Hva med kundenes infrastruktur (brannmurer, sikkerhetsnivået)?

Er det noen krav fra kundene

Vil designet av PunchOut gjøre at enkelte kunder ikke kan benytte seg av PunchOut?

Go shopping

Hva om MP URL er feil?

Er redirection til en annen side mulig

Hvordan er autentiseringen til MP?

Hva skjer når session utløper?

PunchBack:

Kan handlekurven manipuleres?

Kan uønskede hendelser oppstå gjennom MP kontakt med andre servere?

Hva om PunchBack ligger i et annet application domain?

Input sjekking? Hva om noen sender en stor pakke?

Har formatet noe å si for kundenes infrastruktur?

Hvordan håndteres autentiseringen? Er det noen svakheter med autentiseringen?

Falske post? Redirection?

Hva om inboxen er for full?

Kan man poset meldinger fra andre enn MP? E-mail f.eks?

Hente innkjøp:

Sortere på dato
Slette funksjonen

HazOp guidewords

Session hijack: En hacker overtar sesjonen mellom to maskiner

Tampering attack: F.eks endre parametere i en session, endre konfigurasjons settinger, redirige til en annen side, endre brukers rettigheter

Replay attack: En angriper som gjør et angrep på nettverket f.eks lytter på linja og snapper opp passordet for siden å logge seg inn som en annen, eller forsinke trafikken (DOS angrep)

Integrity: Beskytte mot uønsket endring av data. Data ikke blir endret av uautorisererte

Confidentiality: Informasjon ikke er synliggjort for uvedkommede

Availability: data, ressurser e.l er tilgjengelig når en autorisert enhet trenger det.

Authentication: Brukeren er den han utgir seg for å være

SQL injection: Intrenger/bruker kan manipulere databasen

Bufferoverflow: oppstår når man prøver lagre mer data i en buffer enn den er beregnet til å kunne lagre

Avsløring (åpne for noe som har vært skjult)

Vrang forestilling (distortion)

Manipulering

Forsinkelse

Ødeleggelse

Sletting

Utilgjengelig

Frakoblet

Kapasitet

Programerings feil

Korupsjon/forfalskning/bestikkelse

Sammenbrudd

DOS

Bruker feil

Løgn/oppdiktning

(replay) Gjentakelse

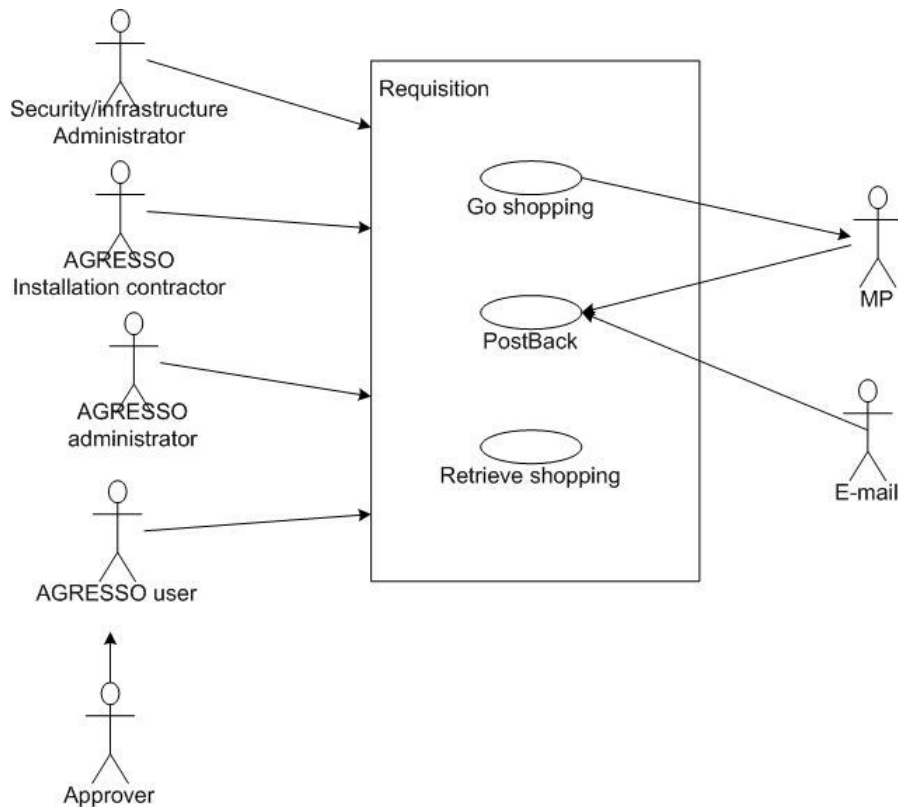
Analysis target

Access points to the AGRESSO POF

When Agresso users should use PunchOut they enter the AGRESSO requisition site. There are several ways to access the requisition site and use the AGRESSO POF. The users are connected to certain roles in AGRESSO.

Figure 26..displays different possible access points to the requisition site:
Security/infrastructure administrator: network configuration, administrate the network.

- *AGRESSO installation contractor*: Installs and configure AGRESSO
- *AGRESSO administrator*: Creates users and roles. Decides who could access Requisition and who approves the purchases.
- *AGRESSO user*: Has access to AGRESSO POF.
- *Approver*: Approves the purchases shopped by the AGRESSO user.
- *Marketplace (MP)*: Place where you can go shopping.
- *E-mail*: Possible to post back purchases from an e-mail client or other types of clients



Communication between the AGRESSO PO components

The AGRESSO POF consists of several components that each has different tasks in the PunchOut process. Figure 27..displays which components that communicates during the AGRESSO PO session.

Component description:

- *PipelineManager*: Gets the predefined pipeline components.
- *ErrorHandler*: Handles the error in the pipliene process and error with the pipeline.
- *MessageInbox*: Contains the purchases that are being posted back from the marketplace.
- *RequisitionSite*: It is the interface that communicates with the user.
- *Marketplace (MP)*: External site where the user shop (e.g. IBX).

