



LAUREA
UNIVERSITY OF APPLIED SCIENCES
Together we are stronger

Charting corporate security in a large enterprise based in Finland through a modified CMMI

Murto Kalle

2017 Leppävaara



Laurea University of Applied Sciences
Leppävaara

**Charting corporate security in a large enterprise based in Finland
through modified CMMI**

Kalle Murto
Degree Programme in Security
Management
Bachelor's Thesis
November, 2017

Kalle Murto

Charting corporate security in a large enterprise based in Finland through modified CMMI			
Year	2017	Pages	72

This thesis was conducted to a large size corporation located in the capital region of Finland. The purpose was to develop the case company's corporate security service. First, it required the mapping of the level of corporate security, after which the situation was monitored in the case company. After gathering of the research material the results were formed.

The thesis was conducted as a qualitative research. Since a strict tie to theory is not a feature of qualitative research, the study does not take advance of a firm way of thought. To clarify the research process, the Capability Maturity Model Integration for Services -maturity model was used as a loose framework. Out of all the model's process areas ten were chosen, and the model was flexibly applied in order to provide more fruitful information.

The study utilized documentation analysis, interviews and observation. The documents were related to the company's security such as memoranda, descriptions, plans and general documents. The interviews consisted of sixteen questions of which six were general questions and ten process area questions. Twelve persons from different levels of the company participated in the interviews, conducted as individual interviews. The observation period was during the year 2016 and consists of the author's entries. Throughout the year 25 entries were produced. In addition, the performance of the company was evaluated with the maturity model.

The results of the study are formed via the methods above. The interviews and observations form a picture on the current state of corporate security and on how it is understood in the case company. Documentation analysis goes through the longer period development of corporate security. The development proposals are presented at the end.

The research results were compared to the process areas and maturity model evaluation. On average, Capability level is - "performing", while Maturity, stays in level one - "Initial". The highest evaluation scores were reached on the following process areas: Work planning, Work Monitoring and Control and Supplier Agreement Management. The Risk Management component was ranked to be the most underdeveloped.

Keywords: Corporate security, Security Development, Security management, CMMI, Capability, Maturity

Kalle Murto

Yritys turvallisuuden kartoittaminen Suomalaisessa suuryrityksessä muokatulla CMMI kypsyyssmallilla

Vuosi 2017 Sivumäärä 72

Tämä tutkimus tehtiin Suomen pääkaupunkiseudulla sijaitsevaan keskisuureen yritykseen. Opinnäytetyön tavoite on kehittää ao. yrityksen yritysturvallisuuspalvelua. Palvelun kehittäminen vaati ensin yritysturvallisuuden tason kartoittamista, jonka jälkeen tilannetta seurattiin yrityksessä. Tutkimusmateriaalin keräysvaiheen jälkeen alkoi tulosten muodostaminen.

Tutkimus suoritettiin laadullisena tutkimuksena. Koska kvalitatiiviselle tutkimukselle ei ole ominaista tiukka teoriasidonnaisuus, tutkimus ei hyödynnä täysin valmista ajatusmallia. Tutkimuksen kulun selkeyttämiseksi löyhänä viitekehysenä työssä toimii Capability Maturity Model Integration for Services -kypsyysmalli. Mallista valikoitiin kymmenen soveltuvaa prosessi-alueetta, ja sitä sovellettiin tutkimuksessa joustavasti, jotta opinnäyte tuottaisi enemmän ja hedelmällisempää tietoa.

Tutkimuksessa hyödynnettiin dokumenttianalyysejä, haastatteluja ja havainnointia. Dokumentit olivat yrityksen turvallisuuteen liittyviä pöytäkirjoja, kuvauksia, suunnitelmia ja yleisiä dokumentteja. Haastattelut koostuvat 16 kysymyksestä, joista kuusi oli yleisiä kysymyksiä ja kymmenen oli prosessialuekysymyksiä. Haastatteluihin osallistui 12 yrityksen eri asemassa työskentelevää tai työskennellyttä henkilöä. Haastattelut toteutettiin yksilöhaastatteluina. Havainnointi tapahtui vuoden 2016 aikana ja koostui tekijän omista muistiinpanoista. Vuoden aikana kertyi yhteensä 25 erillistä kirjausta. Lisäksi yrityksen suoritusta arvioitiin kypsyysmallin avulla.

Tutkimustulokset muodostettiin käyttämällä edellä mainittuja metodeja. Haastattelut ja havainnointi muodostavat kuvan yrityksen nykyisestä tilasta sekä siitä, miten yritysturvallisuus käsitetään yrityksessä. Lisäksi haastatteluissa kysyttiin, miten yritys suoriutuu kypsyysmallin vaatimuksista. Dokumenttianalyyseissä käydään lävitse yritysturvallisuuden pitkäaikaista kehitystä. Lopuksi on esitetty kehitysehdotuksia.

Tutkimustuloksia verrattiin prosessi alueisiin ja kypsyys mallin arviointiin. Keskimäärin Kypsyys taso on - ”Performing”, kun Kypsyys pysyi tasolla yksi - ”Initial”. Korkeimmat arviot saivat seuraavat prosessialueet: työn suunnittelu, työn seuranta ja hallinta ja toimittaja sopimusten hallinta. Riskienhallinta arvioitiin alisuoriutuneimmaksi.

Table of contents

1	Introduction.....	7
2	Theoretical Framework	7
	2.1 Research Questions	9
	2.2 Definitions	9
	2.3 Case company.....	13
3	Methods.....	14
	3.1 Interviews	15
	3.1.1 Questions	16
	3.1.2 Transcribe & Translation	17
	3.2 Observation	17
	3.3 Analyzing documents	18
	3.4 Ethicality and reliability	20
4	Structure of Capability Maturity Model Integration for services.....	21
	4.1 Key components	22
	4.2 Capability Maturity Model Integration for services process areas	23
	4.3 Understanding the Capability Maturity Model Integration	23
	4.4 Viewing process areas & relations of processes	29
	4.5 Optimizing process areas.....	32
5	Results	33
	5.1 Interviews	34
	5.1.1 Definition of corporate security.....	35
	5.1.2 Corporate security responsibilities	36
	5.1.3 Corporate security in business.....	37
	5.2 Observations & documentation analysis	38
	5.2.1 Awakening of security issues	38
	5.2.2 Major corporate security development	39
	5.2.3 Everyday corporate security	41
6	CMMI	42
	6.1 Capability & Maturity level	43
	6.2 Maturity level 2 process areas.....	44
	6.3 Maturity level 3 process areas.....	45
7	Development proposals	47
	7.1 Responsibilities & Strategy	48
	7.2 Risk management.....	49
	7.3 Contingency plan	49
	7.4 Metrics & Monitoring.....	50
	7.5 Incidents management	51

7.6	Implementation of security activities.....	52
7.7	Reflections	53
7.8	Thesis evaluation by the thesis supervisor in the case company	53
	Figures.....	58
	Tables.....	59
	Appendices.....	60

1 Introduction

The purpose of this thesis is to research the development of corporate security service and recognize useful practices to develop it. This thesis was done to a case company which operates mainly in the field of planning and consulting of infrastructure. The thesis was executed as a qualitative study to the case company's corporate security service. The development is researched by using documentation analysis, interviews, and observation. To evaluate the development a measurement system was required. Capability Maturity Model Integration with the author's modification offered a concrete platform to give a level system to measure the corporate security service.

Corporate security is part of every company's functions. Its size and visibility is linked to the area of business and to the size of a company. Establishing corporate security service increases resilience. On one hand, it is passive and might never be needed if a company is lucky enough to never face any security issues. On the other, the future can never be predicted with certainty. One of the interviewees verbalized it well. "Some skipper can sail with poor skills his lifetime without being ever shipwrecked, but it can be just good luck and some good skipper can run shipwreck once in a while." (Interviewee K 2016. Personal communication.)

Corporate security itself contains the risk of becoming rather a burden in bureaucratic and economical form rather than a useful instrument. In the worst case it can realize itself as a cost in a company's budget which does not contribute to the company's operating profit. This rises a reasonable question: Why a company should develop corporate security in the first place and not to accept the current level?

Corporations have different kind of needs for corporate security, and it's crucial to set the correct target level in order to create successful security management system. Companies that decide to be happy with the current situation represent the skipper who has not grounded a ship during his lifetime. Still these skippers are sailing. This thesis aims to offer guidance to those skippers who are willing to improve their skills so that in the time of corporate security breach the horizon is clear.

2 Theoretical Framework

The topic of developing corporate security service was chosen with the case company's representatives. Since 2013 the case company has had a part-time Chief Security Officer (CSO). Though some progress has been achieved, not all the processes are clear or managed as properly as they could be. This situation gave the idea to develop corporate security service. The thesis is at the same time a design research and a development project.

According to Kananen, design research does not have its own methodology and other methodologies are used for development aiming to an objective. Development work converts to a research, when scientific methods, which produce reliable and new knowledge, are applied to the work and documentation. The research has to have a research objective for the development. (Kananen 2013, 20-25).

This thesis is conducted via qualitative methods, and therefore no strict theory is adequate. Qualitative research is free from preconditions and assumptions, which may end up with inventing a new theory from down to top (Eskola & Suoranta 1998, 14-15 and 19). Of course, in order to provide for a clear presentation about the progress of the research, the Capability Maturity Model Integration for services - CMMI - serves as a loose framework. For example, the development proposals in chapter seven for the benefit of the case company are partially based to CMMI. The adjusted CMMI is explained in chapter four.

Nonetheless, qualitative approach allows the object rather speak for itself than try to make it fit a certain given way of thought. In fact, such an open-minded attitude could help the researcher to find wholly new perspectives. The so called “research-related imagination” does not inevitably produce unnecessary information: on the contrary, speculating with possibilities might better reflect the reality than a strict source material-bounden approach (Eskola & al. 1998, 20).

A second advantage of the chosen framework is that it enables a more profound, even triangulate, understanding of the multi-faceted essence of corporate security. As Cabric puts it, corporate security still remains a mystery for many. The role of corporate security contains many controversies and internal conflicts which lead to the misunderstanding of the whole concept (Cabric 2015, xiii). Cabric continues that the attitude towards security as an unnecessary expenditure is slowly changing and the additional value it generates is recognized. Yet, he sees that the “the actual trust and understanding are still missing” (2015, xiii).

The previous statement characterizes the situation in the case company relatively well. E.g. interviewee K compared the state of security management to a state of fermentation. To conduct an effective study in the mentioned state, the CMMI offered a workable platform to analyze and develop corporate security. In total, CMMI for services has 24 process areas out of which ten were chosen with the case company’s CSO. Having selected the most suitable process areas the CMMI evaluation logics were adapted to suit the thesis’s aim. Instead of the rough original ranking, the evaluation scale was softened to be flexible and therefore more informative.

2.1 Research Questions

According to Kananen (2013, 60) there are various models how to conduct a design research, but all of them begin by defining the research problem. The research problem in this thesis was the overall evaluation of the corporate security service and its implementation in the case company.

It's worth noticing that this thesis uses corporate security definitions to define the subject, but it is not researching corporate security itself as a topic. This thesis focuses on corporate security development through a capability & maturity model designed to measure maturity of a service.

The qualitative approach generated three research questions:

- What is the current level of the corporate security service?
- How process areas should be developed?
- How to reach the target level of corporate security service?

First, the initial state of corporate security service in the case company has to be sorted out to have a comprehensive picture of the research object. Identification of the current level of corporate security will be done through analyzing documents, observation and interviews. These form the basis from where to start the development need assessment.

After understanding the current state, the benefits and defects of the process areas can be pinpointed, and development proposals charted. Finally, the results are summed up and realistic aims can be set to develop corporate security service. The recommendations are then presented to the security team of the company, which decides whether to implement or not the proposals.

2.2 Definitions

In this section corporate security service is explained. The following terms are clarified below: *Corporate security*, *Development*, *Service*, *Corporate security development* and *Corporate security service*. Also the corporate security model of the Finnish Confederation of Finnish Industries (EK) is given a deeper review.

The Finnish Confederation of Finnish Industries corporate security model

EK is according to their website (Mitä teemme? 2017) an employer union which operates for the improvement of the business environment for businesses and bolster the services of mem-

ber associations. EK (2016, 2) defines corporate security as follows: Corporate security is safety & security of all the operations and it has five key elements: Personnel, Reputation, Information, Assets and Environment. These are basic assets which are present in every company. However, depending on the company's business operations the emphasis of areas varies. Therefore, every company has its unique needs for corporate security. The functions of the corporate security model and core values are illustrated in Figure 1.



Figure 1: The Finnish Confederation of Finnish Industries corporate security model

Strategy

Corporate security is part of the corporation's quality system and it creates additional value. Therefore, it's beneficial for corporations to commit to the continuous development of corporate security. Standardization, quality and metrics of the corporate security procedures give clear picture from the corporate security activities to the corporation and partners without detailed exhibition (EK 2016, 2-3).

Risk management

The model encourages companies to do a comprehensive risk assessment on security threats and from consequences of the threats in case of they realize. According to the model the recognition of threats, risk assessment and risk management are central preconditions for defining corporate security and measuring it. Security and vulnerability assessments are part

of recognizing threats, evaluating the magnitude of the treats and part of preparing to them. (EK 2016, 2-3).

The EK-model advices corporations to tie central stakeholders and partners to the risk management process. The aim of security measures and risk management is not only to delete and reduce risk, but also give opportunities to the corporation to take risks. (EK 2016, 2-3).

Security leadership & culture

The development of security activities can be established through orientation to statistics on accidents, security deviation and loss & damage. Compiling high-quality security instruction may also develop security activities of a corporation. Creating good security culture, increasing security awareness and training the personnel is very important. It is necessary for a corporation to have leadership and communications system in order to secure the functioning of the corporation in all situations. Feedback from security issues shall be given to the personnel of the corporation and stakeholders and they should be encouraged to notify safety and security in all activities. (EK 2016, 2-3)

Corporate security measures are used to protect corporation's core values. Purpose of corporate security is to ensure the business continuity, enhance competitiveness and improve productivity. According to the definition security management is normal part of the management of a company. The aim is to secure the continuity of the corporation, meaning that all the required standards are met in every situation.

EK has developed a corporate security model which provides for a base to understand corporate security field. An important notification is that the industry area and business model of a corporation steer the importance of different areas of corporate security. The importance of different security fields varies depending on the corporation and business area. Essential is to develop the relevant security fields. The concept of continuous development has been taken into account in the model (EK, 2016, 3).

According to Leppänen (2006, 14-15) the whole of security management includes thousands of actions of personnel and events, and the process of single risk evaluation & management of a single person can be held as a starting point of security management. Corporate security management requires process which takes in consideration the specific features of a company and the requirements to fulfill the role of corporate security management to support the entire business. Security management and operative risk management in all qualitative scales and breakdowns can be built as a supportive process of the business to search, analyze, repair and follow compromising factors. Leppänen (2006, 14-15).

Leppänen (2006, 58) continues that the only correct perspective to security management is the ownership perspective. From this perspective corporate security and security management focus to maximize the return on invested capital. Creating a successful corporate security management system requires knowledge and good understanding of the business the company does. This perspective is reasonable because corporate security is above all a supportive process.

According to Kovacich & Halibozek (2003, 63) *corporate security* and the CSO's tasks are often viewed as a necessary evil. One reason for this is the corporate security perspective which may demand another kind of approach, how processes should work instead of what business has planned. They continue that corporate security is often seen as an overhead cost and does not contribute to the company's profit. Finally, if corporate security is not executed efficiently enough it can be a "parasite on the profits." (Kovacich & Halibozek 2003, 64). This definition has negative approach to corporate security, though it is acceptable and realistic.

It is important to exclude corporate security and security business. While security business is selling security services and equipment in order to gain profit, corporate security is a supportive service or activity which is to secure corporation's key activities.

Service

The definition of service is defined by the CMMI for services as an intangible, non-storable product (2010, 38). Because of the broad definition the model is usable with various sectors of service, including corporate security.

Development

This term is defined by the Cambridge dictionary (Cambridge University Press, 2016) as a process in which someone or something grows or change and becomes more advanced. In this definition, development has two factors growing and changing as one and becoming more advanced as another. Business Dictionary defines development as: "The systematic use of scientific and technical knowledge to meet specific objectives" or requirements" or as "an extension of the theoretical or practical aspects of a concept, design, discovery or invention." (Business dictionary, 2016 defines development).

The first definition has two factors: there are means how to develop through scientific or technical knowledge. The second factor are the specific objectives or requirements. The second definition suggests that development is utilizing already existing concept, design, discovery or invention through extension of aspects the object has. The Cambridge Dictionary definition has a positive expectation for development and it has an objective which is evolving.

This definition may not be used for example when following a scenario and the outcome after a period of time.

The first definition of Business Dictionary includes a goal in the definition, though it is not mentioned. It also states that there is a use of knowledge to meet the set goal. The second definition of the Business Dictionary suggests that there is an existing object or notion which can be processed further through utilizing extension of either theory or practice of the object or notion.

Corporate security development

According to Heljaste, Korkiamäki, Laukkala, Mustonen, Peltonen & Vesterinen (2008) corporate security development is as any process in a company. It requires measurement, control and updating to ensure the effectiveness. The problem of achieving these goals is related to the vast area corporate security contains. Security activities and areas must be identified and developed systematically, and the results must be evaluated, in order to develop security in a meaningful and logical way to protect company's assets from threats. (Heljaste, et al. 2008).

As definition of corporate security above suggests, it is protection of a company's core business, but also an expenditure. Development consist of two factors: growing and changing as one, and becoming more advanced as another. The corporate security development is defined in this thesis as improving a service of which purpose is to protect and enable the core business of a company at reasonable cost.

Corporate security service

In this thesis, corporate security is identified as a supportive service. In other words, corporate security is practiced to contribute to the overall value of a company and its production, but is not the main business of a company. Corporate security service includes procedures and development projects which are executed by the security team.

2.3 Case company

This thesis was conducted in a real company based in Finland. The company could be described as a multidisciplinary one which operates on multiple field of infrastructure providing consultancy and designing services. It has around 500 to 1000 employees. The main business is planning and consultant services. The work is mainly office work including some field work. The field work includes environments such as construction sites, roads and highways, high altitude locations and a variety of terrains.

The case company has appointed a security team which is responsible for corporate security service. The team had six members during the research and was responsible to the support service management team, which included the heads of support services. The team managed corporate security on different fields depending on the role of the team member. The operation of corporate security processes is also one of the team's tasks.

This thesis aims to research how to develop corporate security in a real case company. A disclosure agreement was made about the thesis between the case company and the author to protect the company's economical and security related interests. The company offers an environment to research the phenomenon of corporate security development. The publicity of the case company is not crucial to the research.

3 Methods

This thesis was performed as a qualitative research. Interviews, observation and document analysis were conducted as research methods. In the work corporate security and development of corporate security and the Capability Maturity Model Integration are defined and flexibly applied to the case company analysis.

According to Marshall & Rossman (2011) a researcher can ask practical questions which aim to contribute to the possible solution of the existing problem. In this case, it is what the current level of corporate security is in the case company and how to improve it. A research is expected to generate information which is sufficient and appropriate to answer the research questions, and complies the validity and ethical standards. This is fulfilled by selecting the correct methods and describing the validity and ethical standards. (Marshall & Rossman 2011, 55-61).

Marshall & Rossman (2011, 55-61) refer to Crabtree and Miller, who state that qualitative research is demonstrated in the Shiva's circle of constructivist inquiry, as described in figure 2. In this circle the researcher has to follow the dance, and at the same time stay apart from it. The aim is not to look for an ultimate truth, but discover and interpret the phenomena. The researcher is challenging the incorrect consciousness and providing a more enlightened consciousness (Marshall & Rossman 2011, cited in Crabtree and Miller 1992, 60).

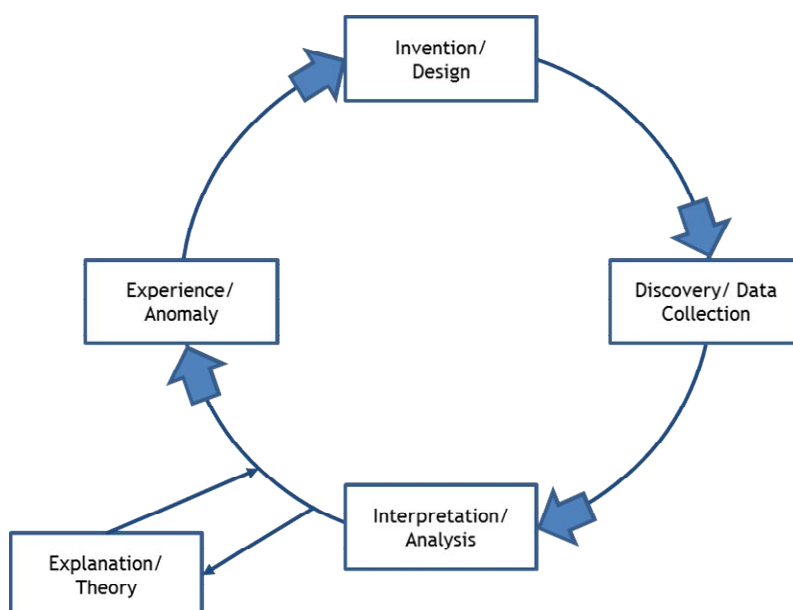


Figure 2: Shiva's circle of constructivist inquiry (Marshall & Rossman 2011, cited in Crabtree and Miller 1992, 60)

The purpose was to use interviews and observation to collect information on the current state of the corporate security in the case company. This information is compared to the maturity model to figure out how the case company manages key processes.

3.1 Interviews

According to Brinkmann & Kvale (2015, 103-109) an interview is a specific context where new information is produced, that separates interviews from other methods. The writers (2015, 103-109) divide interview in to four main aspects: interviewers, interviewees, bodies and the role of gestures as the most crucial part of a interview. This division is made to wake up the researcher's attitude towards interviewing and to see the whole context, instead of just understanding the interview only as a knowledge production tool.

The division and understanding of different context allows the interviewer to understand the impacts of his choices when conducting an interview. For example, the relation with the questions and the topic or the communication of the interviewee and the location, where the interview takes place, all have a correlation which impact to the results of the interview. These factors must be taken in to consideration when planning and executing interviews. (Brinkmann & Kvale 2015, 103-109).

According to Marshall & Rossman (2011, 142-148) qualitative research uses in-depth interviews which should be distinguished e.g. from radio interview. In a radio interview the interviewing is more focused to the width than the depth of the interview compared to a research

interview. In this thesis, the interviews are based on phenomenology. Marshall & Rossman (2011, 142-148) states that phenomenological interviews collect data through the experiences of the interviewee and from how one has understood his/her experiences about the phenomena and developed his/her understanding of the phenomena. Miller and Glassner continue that this approach could open a path to the meanings the interviewees themselves give to their experiences and their social environment (Silverman 1998, 100). The aim is to get description of the phenomena through similar view of multiple interviewees (Marshall & Rossman 2011, 142-148).

According to Marshall & Rossman (2011, 142-148) the interviewees are allowed to prepare for the interview, and the questions are sent beforehand. The interviewer explains the general topic to the interviewee and otherwise respects the answers and structure of the replies. This allows the interviewee to express his/her perspective on the phenomena as it is, and it is not affected by how the interviewer views the phenomena. Though the interviewer sets the topic and interferes as little as possible in to the interviewees' answers, the writer may present follow-up questions to make the interview more fruitful. An interview is often an intimate meeting, and the interviewee might not want to reply with honesty or answers with uncertain replies (Marshall & Rossman 2011, 142-148).

The aim is to acquire qualitative information on how corporate security manifests in the case company. Personnel who at the time of the research were leading in the case company and/or participating security activities was the target group of the interviews. A couple of employees outside the daily corporate security management were interviewed to provide perspective on the corporate security service.

3.1.1 Questions

In total, there were 16 questions which are presented in Appendix 1. The questions were divided in two sections: General questions and Process area questions. General questions aimed to gather general information, views on corporate security and the security culture in the company. Process area questions were specified according to the process areas and aimed to construct identifiable information on how equivalent the company is to the maturity model process areas.

The questions were same for all of the interviewees, and the results were formed question by question, comparing all the answers of one question at a time. The relevant points were picked from the answers to form a conclusion to each question, which was then used to define the capability and the maturity of the case company.

3.1.2 Transcribe & Translation

Since the case company's official language is Finnish, the interviews were in Finnish. According to Marshall & Rossman (2011, 163-168) after transcribing or translation process the information acquired through interviewing transfers from raw data to a processed one. There is an ethical responsibility whilst transcribing and translating. Spoken language varies vastly from the written one: the authors point out that people don't speak in paragraphs or use signal punctuations while talking. The same problem occurs with emotions and visual motions when the records are transcribed. (Marshall & Rossman 2011, 163-168)

The researcher must take in consideration how research participants are presented, how respect towards their contribution is shown, and how to handle the incomplete parts of text, such as half sentences. The commentators recommend that the author should share the transcriptions to the interviewee to confirm that the text carries the purpose and the intentions. (Marshall & Rossman 2011, 163-168).

Due to the problems of interpretation, the translation from one language to another remains a complex process. The authors highlight the term 'interpretation' as the definitions and intents of the world are easily mixed or miss interpreted. Nuances and punctuation from one language rarely translate to another. Using another translator than the researcher complicates the interpretation significantly. (Marshall & Rossman 2011, 163-168).

In this thesis, the interviews represent a significant source of information, especially related to the evaluation of process areas. The interviewees gave a picture on how well different levels of the case company discuss corporate security issues and on the awareness of the top management.

3.2 Observation

According to Marshall & Rossman (2011, 137-141) observation is an essential part of qualitative research. It is used to discover complex activities and relationships. When it is used with interviews, the researcher may verify information by comparing obtained information from interviews and observation. Observation means a systematic monitoring of the phenomena in the social setting. Crucial is to record the notifications.

Marshall & Rossman (2011) continue that at the early stage the researching may be done from a broad perspective. After a while when the researchers starts to observe and discovers patterns in activities and relationships, he may analyze them and focus the observation. (Marshall & Rossman 2011, 137-141). Since the author of this thesis was employed by the case

company for more than a year, and having first hand access to the company's core business, corporate security management and security culture, observation was a reasonable method to use.

Of course, the effect of the researcher's presence can be debated. Field work is an essential way to conduct qualitative research, although it's not compulsory. As Baszanger and Dodier state, the objectivity is secured by remaining open to explore the presentations and normative expectations which people utilize in their interaction with others (Silverman 1998, 9).

In order to scatter the researcher's subjectivities, one must try to recognize his/her own assumptions (Eskola & al. 1998, 17); noticing them enables fresh ideas and viewpoints. In this thesis, the problem of subjectivity was forestalled by making diary entries after important events related to corporate security. Such events were the security team meetings, security related seminars in the company, meetings with the company's CSO or other members of the security team. A couple of general entries were formed to summarize recent events and phenomena. In total, there were 25 entries made during the research period (Appendix 2).

The method gave a thorough overview on the occurring events, but it has weaknesses. Observation is subjective and relies to what the researcher notices. Therefore, it doesn't describe the whole situation comprehensively, because the researcher does not necessary have visibility to all corporate security related organs and the researcher may miss major issues.

The results of the method may be used as a verifier to the information acquired through other methods. From this perspective, the observation contributed to the total evaluation of capability in the case company. It also provided information on pointing out ways to further develop corporate security service, identify best practices for it and map how corporate security service has been developed.

3.3 Analyzing documents

According to Marshall & Rossman (2011, 160-163) organizations and other entities create various artifacts. Documents are one of those artifacts which have been particularly used in qualitative studies. Marshall & Rossman continue that the archival data are the routinely collected information of organizations about official events.

If gathering and analyzing documents is decided to be used as one of the research methods, the records and information should be linked to the research question. Marshall & Rossman (2011, 160-163) state, that the researcher has to be cautious when gathering & analyzing the

documents, because the transparency of the meaning is not present and corroboration of the documents should be verified through other methods.

In this thesis, documents created by the security team of the case company were used for two purpose. First, to validate the information obtained from the interviews and observation and secondly, to obtain via information for the capability and maturity evaluation. Marshall & Rossman (2011, 160-163) continue that while using documents, ethical consideration depends on the availability of the used material. The researcher should consider, whether there is a risk for an exposure or privacy violation. The more classified or private the documents are, the more the researcher has to think about the ethical side of the information.

The security documents of the company add valuable information to the thesis. The documents contain the security team's agendas and memoranda, process descriptions, policies, documentation from projects and memos. With access to the records, there was valuable information available that verified information obtained through other methods.

The case company uses an intranet service, which can be accessed only by authorized persons. Corporate security material has a limited access in the intranet, and it's also used as a workspace to manage documents. During the research period, following documents in Table 1 were analyzed.

Year	Document
2013	Security workshop program & memo
2014	Description of information security
	information security guide for projects
2015	Information security policy
	Creating contingency plan memo
	Process for identifying corporate security needs description
2016	Corporate security policy
	Corporate security objectives and metrics
	Introduction of document classification
	Security introduction training material
	Incident management process description
	Processes and duties of the CSO

2013-2017	Corporate security plan, 2014-2016
	Security team memos, 2013-2016

Table 1: Material used in document analysis

3.4 Ethicality and reliability

According to Kananen (2013, 177-181) a thesis conclusions have to be correct, reliable and credible as should be the results in all research. Kananen states that there are criteria which confirm validity and reliability of a thesis. This criteria represents measurement of the quality of the work, and it has been developed through the science and research process. (Kananen 2013, 177-181)

The information used in the thesis must be examined through objectivity. The thesis should be replicable, which means that the methods used must be explained (Kananen 2013, 177-181). Scientific research is always public knowledge, and criticism towards the results must be practiced in order to overturn the researcher's own conclusions. The thesis as a process aims to create new and most competent information (Kananen 2013, 177-181).

The topic of corporate security itself is a wide area and offers countless research objects. By providing this thesis to the case company, the first limitation is encountered: the company's main business and supportive operations. The modified CMMI model limits the research in to the ten process areas used in this thesis. With these research frames, it is possible to study the subject to a meaningful extent and create new and competent information.

According to Kananen (2013, 177-181) information as itself is only data, but when it is processed through correct methods the information results to creditable data. The information produced must be independent from factors such as economical or religious bonds.

The chosen means provide enough raw data, which is then transformed to credible data through the methods. The independence of the information is safeguarded by following the ethical code of the thesis - any bias which tend to affect the study is blocked. (Kananen 2013, 177-181).

This thesis aims to be neutral and fulfill the above mentioned criteria. When working close to the subject the reliability is under increased pressure to be severed, and the author might develop blind spots or have a conscious or an unconscious bias towards the subject. According to Kananen (2013, 177-181) this phenomenon can be tackled by sufficient amount of documentation.

4 Structure of Capability Maturity Model Integration for services

Capability Maturity Model Integration (CMMI) is an evaluation model developed from capability maturity model (CMM). CMM refers to process improvement approach based on a process model. CMMI was further developed by the Software Engineering Institute (SEI) from CMM to improve the usability of maturity models (What is Capability Maturity Model? (CMM), 2016).

There are three different types of evaluation versions from the model: Development, Service and Acquisition, out of which the Service model is utilized in this thesis. The purpose of CMMI is to improve organizational processes. It includes elements that are essential in order to effectively improve these. (What is Capability Maturity Model Integration? (CMMI), 2016).

According to the CMMI for services (2010, 4) processes hold the system together and researching the processes helps to guide business. Scalability and improving of the processes can be achieved through researching information within the processes.

Structure of CMMI for services was developed to be compatible with the definition of service. The model contains in total 24 process areas, of which 16 are core process areas. One is a shared process area and seven are specific to the Capability Maturity Model Integration for services, including one additional area. In process development CMMI for services points out three critical dimensions of which organizations should focus to improve business. Those three are People, Procedures & Methods and Tools & Equipment, which are marked to the Figure 3. (CMMI for services 2010, 3, 4, 7, 8).

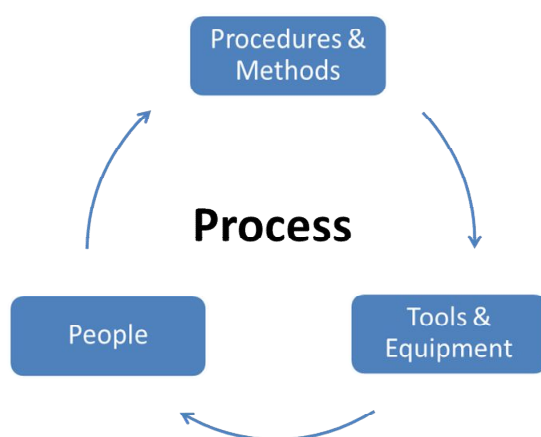


Figure 3: CMMI - three critical dimensions (CMMI for services 2010, 4)

The CMMI provides a workable platform for evaluate and offer development proposals. The model itself has a very strict line, whether, certain processes are defined as incomplete, performed or managed: if there is even one sub-practice notwithstanding, the model ranks the

whole process area as incomplete. As a consequence, the strict evaluation of the model actually prevents the formation of a reasonable view on the current capability and maturity of the case company's corporate security service.

The illustration of the results would be too simplified, and would not serve the purpose of this thesis nor the future development. This problematic situation was resolved by giving certain numeric evaluation to all the sub-practices, and then the overall picture was assessed and ranked. Of course, both of these were conducted in the light of CMMI substance, without using the otherwise too strict ranking model. Finally, to assess the maturity level, all the results were then reflected in relation with the CMMI structure.

4.1 Key components

The CMMI has key components which define how the model functions. The main component is Process area. The process areas are managed with purpose statements, which describe the process area and the factors related to it. These areas are related to each other and this connection is highlighted at the related process area section.

Evaluation of a process area happens through specific and generic goals. These goals are achieved through specific and generic practices which are further divided to sub-practices. (CMMI for services 2010, 9-10). These components create a picture that helps the user to understand practices, processes, goals and informative parts. For their part, they describe important activities and measured targets/themes. The complex system is visualized in Figure 4:

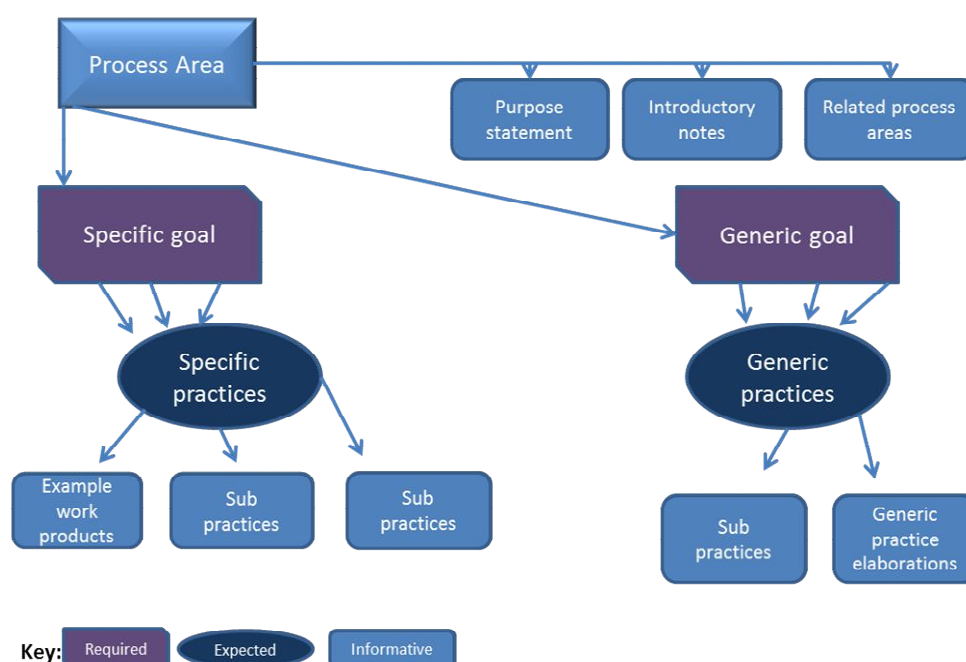


Figure 4: Illustration of the CMMI components (CMMI for services 2010, 10)

4.2 Capability Maturity Model Integration for services process areas

The model has 24 process areas, in which a service can be developed. Has a group of specific and generic practices. These practices have set goals according to which the processes capability and maturity are defined. During implementation of the model the process areas are developed, when all those goals are reached.

Process area:	Abbreviation:	Process area:	Abbreviation:
Capacity and Availability Management	(CAM)	Process and Product Quality Assurance	(PPQA)
Causal Analysis and Resolution	(CAR)	Quantitative Work Management	(QWM)
Configuration Management	(CM)	Requirements Management	(REQM)
Decision Analysis and Resolution	(DAR)	Risk Management	(RSKM)
Incident Resolution and Prevention	(IRP)	Supplier Agreement Management	(SAM)
Integrated Work Management	(IWM)	Service Continuity	(SCON)
Measurement and Analysis	(MA)	Service Delivery	(SD)
Organizational Process Definition	(OPD)	Service System Development	(SSD)
Organizational Process Focus	(OPF)	7 Service System Transition	(SST)
Organizational Performance Management	(OPM)	Strategic Service Management	(STSM)
Organizational Process Performance	(OPP)	Work Monitoring and Control	(WMC)
Organizational Training	(OT)	Work Planning	(WP)

Table 2: Process areas (CMMI for services 2010, 33-34)

4.3 Understanding the Capability Maturity Model Integration

There is no specific order of practices mentioned in the model, and it is up to the user to identify the desired performance. The model demands that there is a process that addresses service related practices. At this stage, the organization can track its processes, while they are mapped to process areas and further evolve or form processes according to the model. (CMMI for services 2010, 21).

CMMI uses an evolutionary level system that organizations can use to advance their services through developing processes. These levels may also be an outcome of evaluations. There are two available improvement paths which are called representations. An organization may improve either process belonging to a particular process area or a group of process areas. On the other path organizations can improve a group of processes linked to each other by developing process areas one after another. The paths are then associated to the representations of levels, i.e. capability and maturity. These two level types are further described “continuous” as “capability levels” and “staged” as “maturity levels”.

To reach a particular level the organization must fulfill all the goals of a particular level of a process area. Both of the methods use the same essential contents, and an organization can improve their service through both representations. (CMMI for services 2010, 21, 22). In the Figure 5 below the focus of the representations of the CMMI is visualized. In the ‘Staged representation’ the maturity levels are used to characterize the relation of the organization’s processes in general. ‘Continuous representation’ aims to characterize the state of the relation of the processes to an individual process area of the organization with capability levels. (CMMI for services 2010, 22).

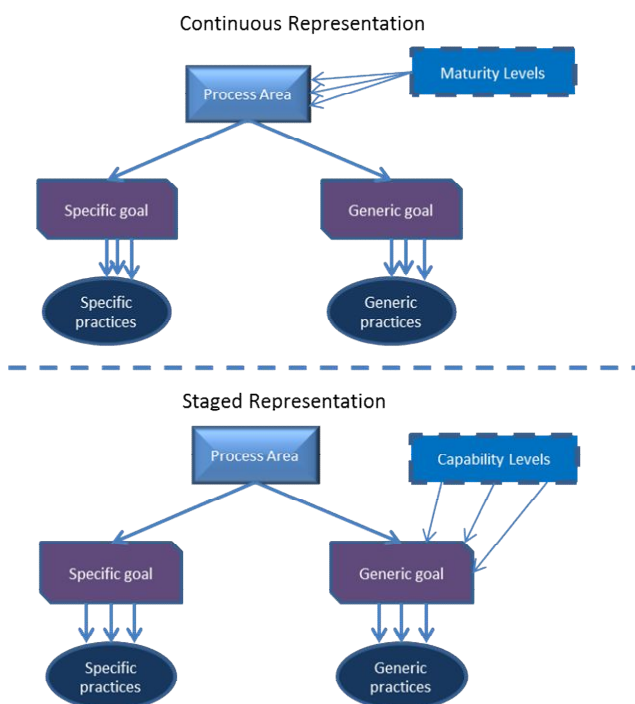


Figure 5 : Continuous & Staged Representation (CMMI for services 2010, 22)

Both representations are very similar. The different dimension comes from the level evaluation system. The capability/maturity dimensions form the benchmarking factors which will guide the organization’s development.

Capability and Maturity levels are measured separately. The capability levels measure development of an individual process area, whereas the maturity levels concentrate in the development of multiple process areas. The model uses a level evaluation scale from zero to five, out of which grades zero to three are capability levels, and one to five stand for maturity levels as in Table 3.

Level	Continuous representation - Capability levels	Staged representation - Maturity levels
Level 0	Incomplete	
Level 1	Performed	Initial
Level 2	Managed	Managed
Level 3	Defined	Defined
Level 4		Quantitatively Managed
Level 5		Optimizing

Table 3: Comparison of Capability and Maturity levels (CMMI for services 2010, 22)

The continuous representation measures particular process area and the desired capability level. Staged representation evaluates multiple processes at once and focuses on the question if processes are being operated. That is why the starting level of maturity levels is Level one, Initial. However, the representations have different approach to the improvement: level two and three have the same definition on both dimensions. This is purposely set, since the same goals and practices are reflected in both of the representations. (CMMI for services 2010, 23).

Understanding Capability Levels

Capability levels define the level of a single process area. A capability level is achieved when generic goals of a certain level are fulfilled. Continuous representation of process area is measured with capability levels. The stages of capability levels are from zero to three, or in words, incomplete, performed, managed and defined. Process areas, which are not executed or they are not completely running, are defined as incomplete processes.

Capability level requirements are presented in the following as they're described by the CMMI. Since they were flexibly applied to the evaluation, they offered a fruitful and wide approach to security matters. And taking in consideration the general situation in the case company, Capability level 3 was noticed in the assessment, but never reached.

Capability Level 0: Incomplete process is defined as:

- Process is not performed or is only partially performed
- Process areas have specific goals which have not been fulfilled

- No generic goals because it's not reasonable to establish partially performed process

Capability Level 1: Performed process is defined as:

- Process is considered a performed one
- The process produce work which fulfils the set specific goals of the process area
- Capability level 1 is reached when the required processes of the process area are performed

On the next levels the process involves relevant stakeholders, and it's executed according to a policy with a plan. Standardization of processes evolves constantly. Employees with required skills and adequate resources are responsible for monitoring, controlling, and reviewing the process. The process is evaluated according to the description of the process. The preconditions for capability levels two and three are summarized below. (CMMI for services 2010, 24-25).

Capability Level 2: Managed process is defined as:

- Performed process and planned process
- Process follows a policy that indicates how it will be performed
- Resources are provided
- Responsibilities are assigned
- Training to perform the process is provided
- Selected work products related to performing the process are controlled

Capability Level 3: Defined process is defined as:

- The process is a managed process
- The process area is tailored by organization's tailoring guidelines
- The process description is maintained
- Process related assets are contributed to the organizational process assets

Understanding Maturity levels

Maturity levels are evaluated on process areas, which are predefined, and they consist of generic practices. The process areas aim to improve the organization's overall performance. This performance can be characterized through maturity levels. An achieved maturity level sets important subset for the organization to achieve the next maturity level. The five maturity levels are: 1. Initial, 2. Managed, 3. Defined, 4. Quantitatively Managed, 5. Optimizing. (CMMI for services 2010, 26).

Maturity Level 1: Initial level processes are defined as:

- Usually ad hoc and chaotic
- Lacking stable environment supporting the processes
- Success depends on the competence of staff, not on established processes
- Organization provides service which functions
- Budget and schedule are often exceeded
- Tendency to over commitment
- Processes are abandoned in the time of crisis
- Unable to repeat success

Maturity Level 2: Managed level processes are defined as:

- Organization is an effective service provider
- Project and work management, support, and service establishment and delivery processes are institutionalized
- The process has service strategy, work plans, monitor and control procedures for the work to ensure the service delivery
- Established customer agreements, management of customer requirements and constant development of agreements
- Process and product quality are institutionalized
- Capability is measured and performance analyzed
- Following objects are managed: work groups, work activities, processes, work products and services
- The processes are planned according to the organization's policy
- Adequate resources are provided, responsibilities are assigned, training is given as needed to execute the process and work product match the required quality
- Relevant stakeholders are identified and involved
- The process is periodically monitored and controlled
- Adherence and performance of the process is periodically evaluated and reviewed with senior management

Maturity Level 3: Defined level processes are defined as:

- Defined processes are used for managing work
- Service continuity and incident resolution and prevention are part of the standard process set
- Selected work products are verified to meet their requirements to validate the service
- The processes are understood and described in standards, procedures, tools, and methods
- The organization's set of standard processes, which are used to establish logical processes across the organization, are created

- Work groups establish their defined processes by tailoring the organization's set of standard processes according to tailoring guidelines

Essential differences between the maturity levels two and three are the common standards on process descriptions and procedures, while on maturity level two the processes may have their own standards. Other major difference is the accuracy of obligatory descriptions among maturity levels. The maturity level three especially requires: the purpose, inputs, entry criteria, activities, roles, measures, verification steps, outputs and exit criteria. (CMMI for services 2010, 27-28).

Maturity Level 4: Quantitatively Managed level processes are defined as:

- Quantitative objectives for quality and process performance
- Base for the objectives is defined by the needs of the customer, end users, organization and process implementers
- The quality and performance of process is managed through process lifecycle and it is understood in statistical terms
- Quantitative data from process performance of selected sub-processes is collected and analyzed

The difference between the maturity levels three and four is that on the level four the processes are managed by using statistical data and analyzing the quantitative data. This partially predicts how the process will perform.

Maturity Level 5: Optimizing level processes are defined as:

- Processes are continually improved
- Business objectives and performance needs are understood
- Variation in the processes and the process outcome are understood from the perspective of quantitative data
- Continuous process improvement through incremental and innovative process and technological improvements
- Quality and process performance objectives are established according to the organizational standards
- Processes are revised periodically to reflect changes in business objectives or in organizational performance
- Measurement is conducted to deploy process improvements and their effects
- Statistical and other quantitative techniques are used and compared to quality and process performance objectives
- Target stage is to have defined processes, organization's set of standard processes, and supporting technology which are measured

The difference between the levels four and five is related to the progress of organizational improvement. On level four the improvement focuses on the sub-processes, while on level five the focus falls on the overall performance of the organization.

In a wider picture, improvement happens when requirements on single process areas are fulfilled. Maturity level advances mark the assumption of quality in the work. As an example, work on maturity level one is ad hoc, whereas on level two the work is managed via a planned procedure, and the required resources are available. (CMMI for Services 2010, 28-30).

4.4 Viewing process areas & relations of processes

Process areas are viewed differently depending on the representation. The continuous representation helps to develop singular selected process areas within the process area. When looking at the staged representation, it shows which process areas should be developed in order to achieve the next maturity level. It's important to note that if the maturity level of a certain process area needs to be evolved, then the associated process areas must also be taken in to consideration. The continuous representation divides process areas in four categories: Process Management, Project & Work Management, Service Establishment & Delivery and Support. The categories are used to highlight the relations of the process areas, and they help to shape their development.

When an organization wants to evolve, it has two possibilities. Either focus on development on singular process area to achieve higher capability level, or to develop multiple process areas simultaneously to reach higher maturity level. The evolution is done with target profiles. These target profiles consist of the selected process areas and of the desired capability and maturity levels. The target profiles are later on arranged in to a order which is called *target staging*. This helps the organization to plan and manage the development process. (CMMI for service, 2010, 32).

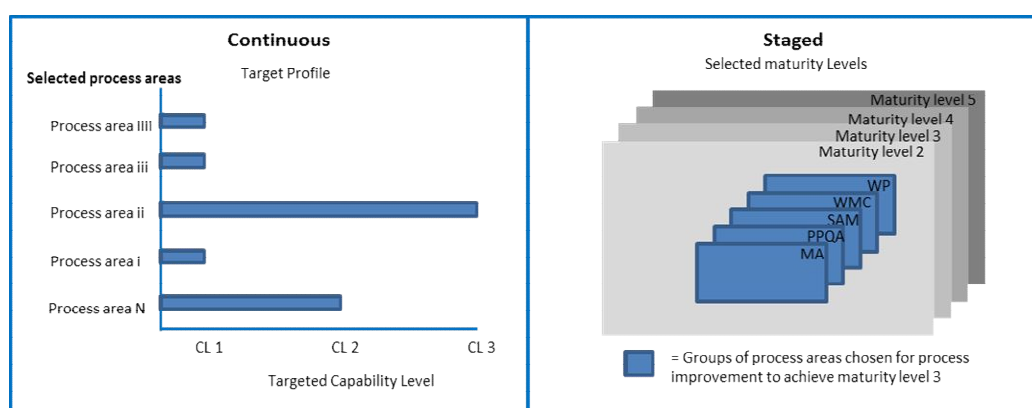


Figure 6: Continuous & Staged preview (CMMI for service, 2010, 32)

The model uses generic goals and practices to define the continuous level of a process area. The aim is to institutionalize generic practices in order to ensure that the practices are executed effectively. Generic practices portray the institutionalization through executed activities. The level of institutionalization is described according to achieved generic goals as in Table 4.

Generic Goal level	Progression of processes	Generic Practices by generic goal level
GG 1	Performed process	GP 1.1 Perform Specific Practices
GG 2	Managed process	GP 2.1 Establish an Organizational Policy GP 2.2 Plan the Process GP 2.3 Provide Resources GP 2.4 Assign Responsibility GP 2.5 Train People GP 2.6 Control Work Products GP 2.7 Identify and Involve Relevant Stakeholders GP 2.8 Monitor and Control the Process GP 2.9 Objectively Evaluate Adherence GP 2.10 Review Status with Higher Level Management
GG 3	Defined process	GP 3.1 Establish a Defined Process GP 3.2 Collect Process Related Experiences

Table 4: Generic Goals & Practices (CMMI for service, 2010, 57)

Following description explains the institutionalization of process progression. Generic goals are contented according to how generic practices are fulfilled. (CMMI for service, 2010, 57, 60).

Performed process

A performed process accomplishes the minimum requirements to satisfy specific goals of the process area. (CMMI for service, 2010, 57)

Generic goals for performed process area:

- Achieving the specific goals of the process area

Managed process

A managed process is a performed process which is “planned and executed in accordance with policy; employs skilled people having adequate resources to produce controlled outputs; involves relevant stakeholders; is monitored, controlled, and reviewed; and is evaluated for adherence to its process description.” (CMMI for service 2010, 58).

The process can be institutionalized by an organizational actor. Specific objectives such as cost, schedule, and quality are institutionalized & defined by the management of the process. When a managed process is controlled, it acquires resilience in state of stress. The organization is responsible to establish the requirements and objectives of the process. The service is available for inspection by management at specified points, for example at milestones or at the completion of a project. Commitment of the staff working with the process and stakeholders is necessary. The labor productions must be controlled and reviewed with relevant stakeholders. The service is required to satisfy its specified requirements. (CMMI for service 2010, 58).

Generic goals for managed process area:

- Manage the execution of processes associated with the process area
- The process is performed according to an existing policy
- The process is performed by a plan
- Resources are provided
- Responsible personnel are assigned
- Personnel executing are trained to perform it
- Services from providing the process are controlled

In other words, the process is planned and monitored. (CMMI for service 2010, 59).

Defined process

The CMMI defines a defined process as following: “A defined process is a managed process that is tailored from the organization’s set of standard processes according to the organization’s tailoring guidelines; has a maintained process description; and contributes process related experiences to the organizational process assets”. (CMMI for service 2010, 58). A defined process encompasses following factors: purpose, inputs, entry criteria, activities, roles, measures, verification steps, outputs and exit criteria.

Articles which are used to describe implementing and improving processes are called *organizational process assets*. The articles are results of the organization’s investments which are expected to create value; they can be identified as assets. The organization holds set of standard processes. Those processes are the basis for defined processes, and are expected to

improve over time and describe the relation between process elements. A defined process has two generic goals which are shown below. (CMMI for service 2010, 58).

Generic goals for a defined process area:

- Existing organizational standard process which can be tailored to be used in different process areas.
- Using the standard process may not need changes in order to work

Relations of the processes

There are several factors which separate a performed process, a managed process and the defined one. First of all, it is the extent of the management. Managed processes have a plan, they are executed by that plan and they achieve the objectives, while the process is institutionalized for consequent performance. A performed process only achieves specific goals of a process area. The distinction between a managed and a defined process is that the defined process has a broader scope in the description of the process, such as the standards and procedures. (CMMI for service 2010, 58, 59).

The managed processes are not as detailed, and do not manifest as punctually. The defined processes are better managed, because they produce information about the interrelationships of the process activities. This provides information on the detailed measures of the process and on the service. The processes evolve according achieved generic goals. Generic goals also describe the processes and mark the phase of institutionalization of the evolving processes from a performed towards a defined one. (CMMI for service 2010, 58, 59).

4.5 Optimizing process areas

In this thesis, the modified CMMI is used to evaluate the maturity of the case company's corporate security and to outline development proposals. Since CMMI carries a software development approach, and considering the size of the corporate security service in the case company, the use of all the process areas was unnecessary. With the company's CSO we decided to use ten process areas to evaluate the maturity and capability of the corporate security service.

As already explained in Chapter 3, the maturity assessment is based on the vast research data. This enables further discussion and reflection about the case company's development needs. The evaluation itself was conducted with numerical scaling to simplify the whole process. The generic goals and generic practices were evaluated individually according to the CMMI as incomplete, performed or managed.

Hence the tripartite scale would only lead to an apparently cruel distinction between the levels, bypassing the development/trends within them, an intra-level analysis was conducted too. As previously explained, the generic goals contain generic practices which are the same in every process area, while the specific goals contain specific practices that vary according to the process area. Judging by the results obtained, none of the process areas reached Maturity level three, so it does not exist in table diagrams nor in results. Nevertheless, to give a comprehensive picture of the Maturity levels and components belonging to them, they are all introduced below.

Maturity level 1 “Initial”

- *No components*

Maturity level 2 “Managed” process areas

- Measurement and analysis
- Process and product quality assurance
- Supplier agreement management
- Work monitoring and control
- Work planning

Maturity level 3 “Defined” process areas

- Capability and Availability Management
- Incident Resolution and Prevention
- Integrated Work Management
- Organizational Process Definition
- Risk Management

Maturity level 4 “Quantitatively Managed” process areas

- Organizational process performance
- Quantitative work management

Maturity level 5 “Optimizing” process areas

- Casual analysis and resolution
- Organizational performance management.

5 Results

The results of this thesis are obtained through the used methods. The interviews, case company’s artifacts and observation together form an information basis. It was then compared to the process areas and maturity model evaluation, although the results gave more substance

to the security management point of view. The observation gave more information related to the Capability and Maturity evaluation, because the performed processes and activities were under the monitoring, and could later on be compared to the requirements of the CMMI.

One aspect was to evaluate the impact of security development to the business. This is because security is a supportive action and not the main business itself. Documentation analysis gave sight on the whole development arch of corporate security and on how corporate security service is executed in the case company.

The interview results are presented first, and then the summaries of answers to the questions are introduced. Secondly, the results of documentation analysis are shown. Thirdly, the findings of observations are presented. To conclude, CMMI results are presented combining some of the results obtained through other research methods.

5.1 Interviews

Background of the interviewees varied a lot. All the interviewees were at least heads of department, members of the security team or the top management. Ten out of twelve had work experience with security before their current position. The longest service period in the case company among the interviewees was sixteen years, and at the shortest a year. The average service year was seven and two months by the time the interviews were recorded. Four of the interviewees represented the top management, and eight the middle management.

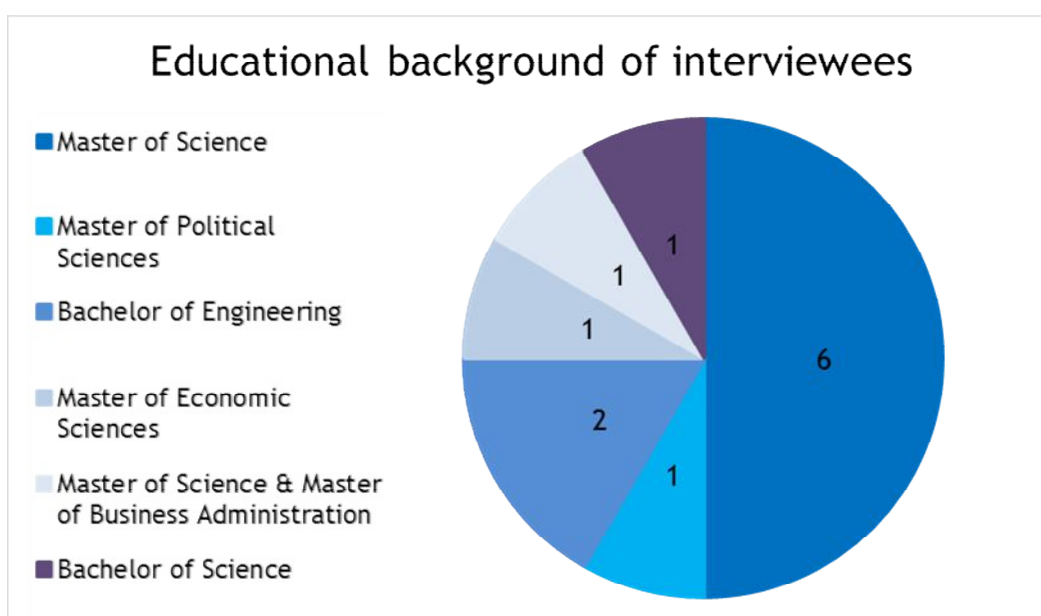


Table 5: Educational background of interviewees

5.1.1 Definition of corporate security

When asked to describe corporate security, all of the interviewees used relatively short definitions. All of the interviewees mentioned key terms which could be divided into 18 security related categories, and the four most mentioned topics were: *Estate*, *Functions*, *Information* and *Personnel*. The result reflects, what the interviewees see as important topics related to corporate security.

To summarize, the physical location where the actual work happens, has a big priority. Well managed estates are important to enable efficient work. However, estate security is a relatively traditional and passive security, which indicates that the case company is still in the beginning of steps to develop security. On the other hand, considering the field where the case company works, there are not many other major disruption factors to the basic work than offices which cannot be utilized.

Information relates to all information security mentioned. It is another key factor of the company, and the majority of the work is consultation and produced with computers. The company has to maintain a relatively big information technology infrastructure. It's no surprise that information is mentioned by most of the interviewees.

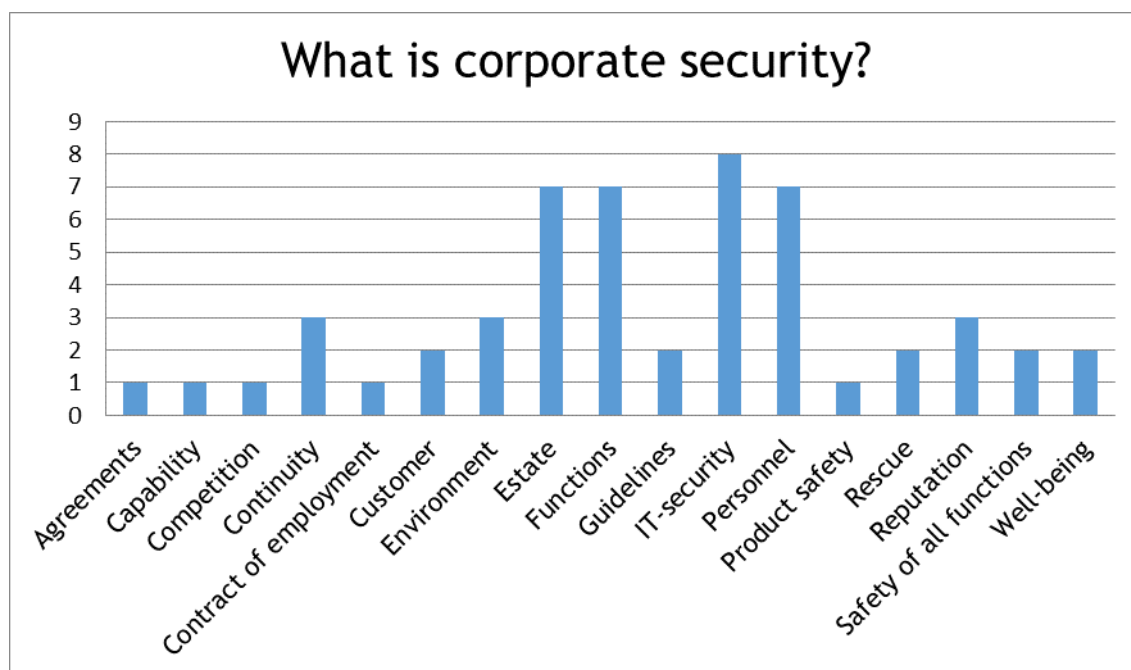


Table 6: What is corporate security?

Functions relate to security functions which are operated in the case company. Security functions is a difficult term, since every interviewee has his/her own idea about the specific secu-

urity function. Generally, it can be understood to indicate that the interviewees recognize the existence and the importance of corporate security.

Personnel was one of the most mentioned topics and it is a major asset for the company. The well-being and safety of the personnel is a set priority which can be explained due to the nature of the company's core business.

What sticks out, is what is absent. E.g. *Risk management* was relatively often mentioned throughout some of the interviews, but it is remarkable that no one mentioned it when describing corporate security. Concepts such as *Continuity*, *Product safety* and *Reputation* were mentioned, but they did not stand out as popular. One could say that they are more specific categories than the four most commonly mentioned. After all, the data shows that the overall understanding of security is somewhat evolved.

Since corporate security can be defined very widely, the key terms were used to form a table (Table 6) which demonstrate how widely or similarly the interviewees highlight different elements of corporate security. Overall, the answers were coherent indicating that the interviewees have similar understanding on what corporate security is, though some answers were relatively short and less informative. It's also worth mentioning that the comprehensiveness of corporate security was mentioned only by a few interviewees. Yet, most of the interviewees recognized the scale of the topic.

5.1.2 Corporate security responsibilities

The responsibilities structure of security management seems to be well acknowledged. The awareness on how responsibility is divided among the whole organization seems to be relatively narrow.

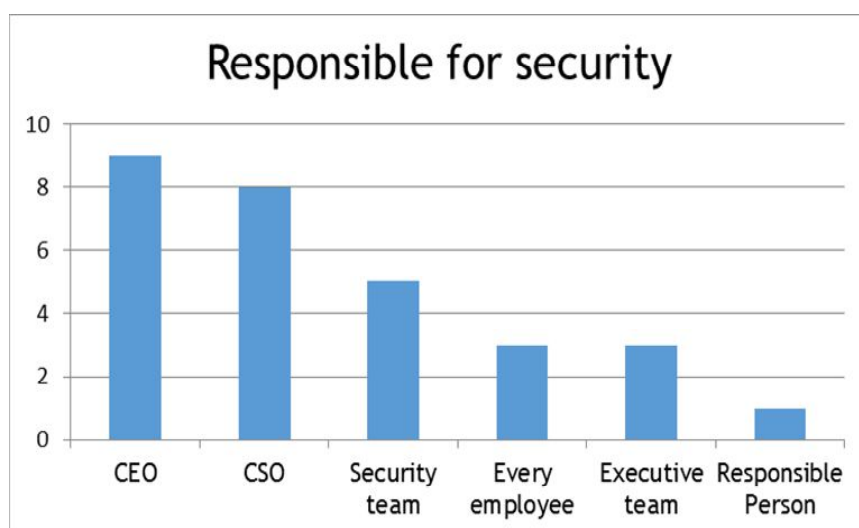


Table 7: Responsible for security

CEO and CSO were much more often named as responsible for security compared to every employee or executive team. This resonates with the idea of knowing who is responsible in organizational structure, but misses the substance of responsibility. Indeed, the CEO and CSO are the responsible ones, if there is a major incident followed by a prosecution. The ordinary employee still has the responsibility to follow security guidelines.

5.1.3 Corporate security in business

The position of the interviewees shaped the answers heavily. A clear trend is that corporate security has become more present than earlier. The commitment of the top management was seen as the leading sign to develop corporate security.

The security management system was established, and a unified thinking on corporate security was emerging. The overall security remains somewhat absent. The possibilities of corporate security is recognized by some of the interviewees, pointing out that it is not only performed to tackle problems, but it also may help to take controlled risks.

Practical examples on how corporate security influences the business are mentioned: *Guidelines*, *Occupational Health & Safety gear*, *Risk Management* and *Commute Travel Safety* to name a few. Security activities and requirements have also been increasing for most of the mentioned aspects are more supportive services than business fields.

Some of the interviewees had difficulties recognizing corporate security's impact to business. One interviewee took up the customers' point of view and named reliability, quality and good service as the outcome of the case company's security measures. *Risk management* was brought up as an important factor, since the business risks were relatively often assessed.

In general, the employees were clearly becoming more informed about corporate security, and security issues seemed to be better managed in the project work. Some interviewees seemed to trust that employees were well aware of the security guidelines and followed them. It seems that there are various security methods in use among different sub-industries, which are nonetheless supervised by the security team.

There were clearly two opinions on the visibility of corporate security. One wished that it could be more visible in the daily operations, because the overall security management was less visible. Corporate security was also seen as a restrictive thing in a positive light from the support service's point of view, but not every employee see it positively. One thought was that when it is not visible, but still present, it would be ideal. There were also opinions that the business should not be disrupted too much by the security measures.

5.2 Observations & documentation analysis

The corporation security functions were monitored throughout the year 2016, while documentation analysis consisted of material from 2013 to 2016. The observation and documentation analysis were combined in the results section. Since these methods produced similar results, it was reasonable to handle both in the same chapter.

The combined analysis offered a suitable information to generate an overall picture. On one hand, the documents conserve a general history of corporate security matters. On the other, especially the security team meeting memoranda provided a informative source to verify the corporate security service procedures. The documents also brought additional information for comparison of the company's current state to the requirements of the maturity model. Observation worked as a verification tool. It is notable that observation was applied only in 2016 to security team meetings.

The company has a functioning information management system regarding security management. It has somewhat messy structure, even though many important documents were maintained, and they contained valuable information. During the observation the amount of security related memoranda and saved documents grew. This indicates recent tendencies of corporate security development, e.g. serious efforts to consolidate corporate security can be noticed from the emerge of information security policy & the Corporate security policies.

5.2.1 Awakening of security issues

The beginning of corporate security development dates back to the year 2013. A security workshop was held at the beginning of November 2013. Background information for the workshop states:

- There is no regular security system
- There is no well-organized security team
- Security mapping is needed
- Establishment of corporate security development plan
- Eleven point program

The top management and stakeholder group representatives were comprehensively present in the workshop. In the workshop, it became clear that the case company had to take a stand on corporate security issues. The basic elements of the corporate security were agreed, a corporate security team was established and the first security metrics were established, including ten measurable points with a scaling 'executed' / 'not executed'.

After the workshop, the corporate security team held its first meeting in December 2013. The basic corporate security responsibilities were assigned, the corporate security team was established and other security relative issues were discussed. These comprised document classification issues, work habits of the corporate security team and security incidents. Furthermore, starting from 2013 a security plan is drafted and executed annually.

Year 2014 had a heavy emphasis on practical security & information security. Topics, that occur in the documents, were for example creation of information security policy, composing security attachments and mapping information security threats. An information security description, including several components, was formed alike, while information security instructions were set to be drafted.

From the memoranda of the security team it can be noticed that the security development focused vastly on practical corporate security. This trend was obvious, because 2014 was the first full year of corporate security development. During this period the working habits of the security team started to form. As a testimony for the enlargement (and an increasing understanding?) of corporate security, in 2014 risk management, contingency planning, crisis management and security policy were all added to the yearly security plan.

Throughout the following years security plans were seemingly better established, having different security sections named, and development objectives set underneath. Still, the accent fell mostly into information security. Overall, 2015 became the year of establishing the corporate security service, defining key procedures and binding relations with key stakeholders. Notable is the decrease in the amount of security team meetings, from nine to six during the year.

The establishing of the service and indistinct working methods probably explain the decrease in the amount of meetings. Two remarkable things also rise from the documentation of 2015. For the first time since the security workshop in 2013, security metrics are mentioned in the security plan for the year 2016, and a memo is composed to establish a contingency plan. During the observations, security metrics were a well discussed theme, however, the decision making on the subject stumbled.

5.2.2 Major corporate security development

Year 2016 brought the institutionalization of corporate security service. The new corporate security policy entered into force, but required harmonizing in security issues. This policy defined objectives, principles, roles, responsibilities, security aims and metrics of corporate security. It had a stand on risk assessment, follow-up and surveillance. *Process for identifying*

corporate security needs description was created to help the security team to tackle the problem of individuals giving subjective descriptions of the case company's corporate security settings. The team was also worried about security incidents which never came to the team's awareness, or about customer requests to business concerning corporate security, which either were described by the employees themselves or were brought to attention just slightly before the return date.

At the first quarter of the year there were major events such as the risk workshops, changes in the security team personnel. After a relatively busy spring a new CSO was appointed in June. The autumn started with the handling of several security incidents and an ad hoc request from top management. Towards the end of the year security management improved, as can be observed from the security team meeting topics and decisions. The last entry from December summarise the then state of corporate security and points out development needs. It also records the CSO's desire for additional resources to corporate security work.

With an outside service provider the case company initiated risk management process during the spring of 2016. It consisted of workshops and a risk management tool. Considering the commitment to the risk management process it can be said that the case company took an enormous step within this area, although the workshop handled broader topics than corporate security. From the observation it rises that the initiation of risk seminars is related to the company's objective to achieve a quality standard, i.e. the lever balances between the pragmatic approach and voluntary willingness of the top management to improve corporate security. The top management approach was a pragmatic one, which saw the quality standard as an external standing order. There remained at least one continuous reason to initiate and upkeep the risk management process. Certain members of the security team felt that this workshop didn't provide much information about risks of their own field, and that the process should be deployed to lower levels in order to meet the corporate security needs.

Security metrics, which was another visible development area, was much more detailed for the upcoming year 2017. It included four categories with nine subcategories to be measured. Additionally, a few numerical metrics were established for the first time. The metrics were further developed throughout the year. The development of the metrics were not progressing due to lack of attention and the mutual expectations of the top management and security team. There were also unclerness in the roles of single employees and even organs. E.g. there was a decision that the Support Services Management Team (SSMT) would start to follow a security metric which was already being followed by the security team. While observing, this was a sort of managerial problem. A singular metric was addressed, instead of advancing the whole security measurement.

5.2.3 Everyday corporate security

Since 2014 the case company had been arranging security trainings to new employees, and during the early stages of the year 2016 the training material was reviewed and updated. The new version included five sections: Security objectives of the company, Estate safety & security, Information security, Emergency procedures and Acquiring security assistance. The security management system itself had a general description, but the smaller elements were not defined as well.

Incident management had been developed vastly since the second half of the year 2015, and this materialized into an *Incident management process description*. The security team memoranda clearly demonstrate an annual growth in the amount of reported and handled incidents. The increase in the awareness of incident management, recording of incidents reported orally or via other unofficial means, and the change in perception of an incident can be named as reasons for the upward trend. Nonetheless, there were still incidents which did not reach the attention of the corporate security team.

During the second quarter of the year 2016 the security team had personnel changes, including the Chief Security Officer. This affected the work of the security team, and it was decided that the security team will not be summoned until the new CSO is appointed. This generated a serious question: Who will substitute the CSO? Recruitment of a new CSO was initiated soon after the incumbent resigned, and as an advantage of this period was that the duties and processes of the CSO were defined. By the end of the year the security activities were again managed properly.

The documentation classification had for a long time been under formation alike. The top management and the security team had long discussed the issue, but little progress was achieved. During the year 2016 the need for the documentation classification procedures grew, and an introductory guideline was formed. The document classification was not taken into use during the research period. It remains a question whether a document classification procedure is established.

During 2016 the security team had five meetings. The still decreasing trend of security team meetings can be explained by the personnel changes. Thus, the information was more fruitful. Throughout the year document classification was a discussed topic, escalating to a top management request to deliver a functioning process description by the end of the year. This was due to a customer request, and this kind of security development pictures well how corporate security is being developed in the case company. Again, corporate security develop-

ment is not high on priorities until a customer demand is presented. Only then, the top management activates and requires the security team to respond to the respective case.

Though the harsh expression, in turn the top management is open for the corporate security development outside the active needs. This may indicate that the additional value and need for corporate security are recognized in the top management. Albeit willing, the top management was more pragmatic to develop corporate security. It also had doubts about the importance of corporate security development and its role. It seems that Leppänen is right when he depicts the pragmatic, even cynical, ownership perspective on corporate security. The security team was more aware of the deficiencies of the corporate security and had a better vision of the development, but were lacking resources and the top management's engagement.

An outside occupational health & safety inspection was executed to one of the county offices of the case company by respective officials. The inspection itself went well, but it woke confusion in the security team's responsibilities, relating to who represents the occupational health & safety manager in the case company. Though inconsistent, is a minor one, yet it underlines need for a clearer division of labor.

6 CMMI

The process areas were evaluated by the author and the Chief Security Officer. The author's answers are based on used research methods, while the CSO's evaluation bases on his own experience, and was acquired to have a reflective view on how the case company performs. The CSO's task is a key position, enabling the best view to understand corporate security, and the opinions of the CSO gave valuable comparative information.

The results of both generic and specific goals were formed through a grading system. First, the specific practices were evaluated as executed/non-executed. Later, the overall amount of executed VS non-executed practices were summed up, and this defined if a generic or specific goal is complete (or in numbers 2), partially complete (1), or incomplete (0). Then the summary of graded goals were divided by the amount of the goals, which gave the final grade for the total process area. The final grades are rounded, and differ a little bit, hence the amount of specific goals varies between the process areas, whilst every process area has the same amount of generic goals (Appendix 4).

Every generic practice of each process area was evaluated one by one and given a numeric grade. Of course, to keep it reasonable, only fractions that can be divided with three (rounded as 0,3 and 0,7...) were applied to. Apart from serving the purpose of the thesis better, the

intra-level analysis gave a more realistic insight to the process areas themselves. For example, even in the case of a fair progress in regards to specific practices, the process area as a whole might still not rank high. As in the case of *Process and Product Quality Assurance*, even with 4/4/2 completed generic practices of the generic goal 2, the final grade resulted in 0,6.

The maturity evaluation was then formed from the assessment of the capability evaluation compared to the entire research data. The evaluations were made in December 2016 and January 2017. An advantage of this was that the CSO was appointed recently and possessed a rather critical attitude.

The evaluation of the Chief Security Officer and the author somewhat crossed, but in general the evaluations were convergent. The CSO had a slightly positive evaluation, while the author evaluated some process areas being more established and others less established. This could be explained by the period of time the two had been working with corporate security. Also, the work experience should not be underestimated pointing out that the CSO has previous experience from conducting quality evaluations. Likewise, the CSO had the main responsibility for corporate security, and a better vision on the overall situation. The author's experience about corporate security, though working with corporate security as his main task, may have been closer to a service user's position.

6.1 Capability & Maturity level

From the Capability's point of view, the case company is "performing" on all the measured process areas. However, the sophistication of the operations varies, and each process area is more precisely discussed below. On average, Capability level of the case company resulted in 1 or "Initial".

When it comes to Maturity, the company usually entrenches level 1 - "Initial". Yet, the following Maturity is reached only when all the components surpass the earlier level. In this case, there's a minor question, which one of the estimates about Process and Product Quality Assurance better reflects the reality.

Whilst speaking of Maturity level three components, certainly two of them obtained Maturity level "Initial". At three process areas there's a notable discrepancy between the author's and the CSO's opinions. The most striking result is the imminently low grade of Risk Management component. The main reason for this could be that the process was initiated only in 2016. Also, the process was prevalently launched for the use of top management, and it remains open if the security team can utilize the process. The deeper discussion follows after Maturity level 2 analysis.

6.2 Maturity level 2 process areas

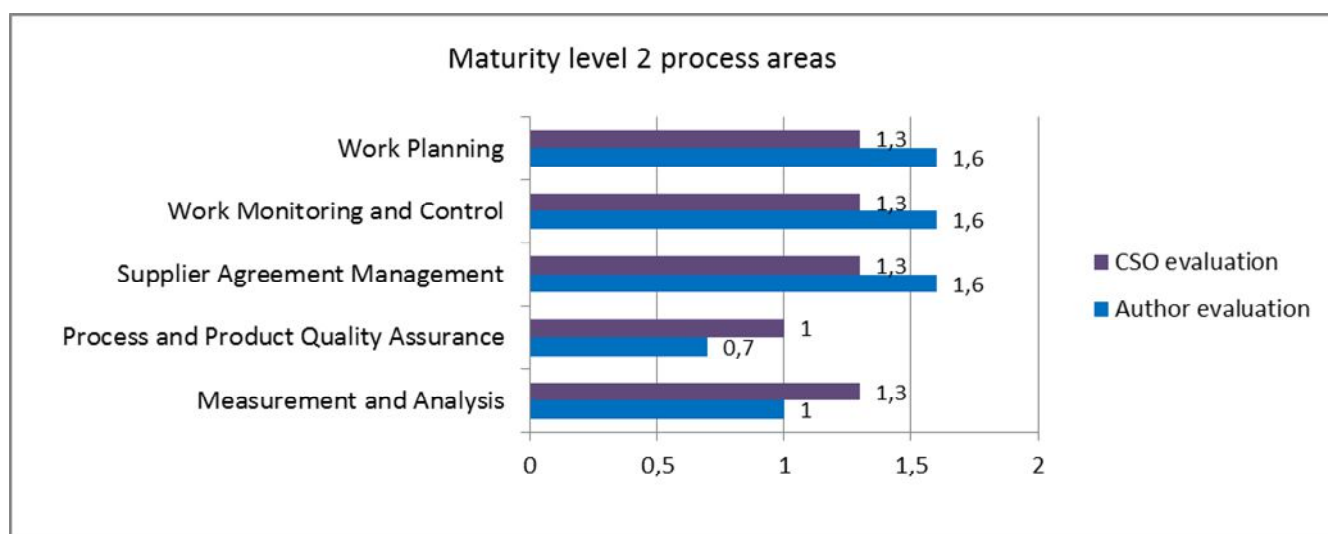


Table 8: Maturity level 2 process areas

Measurement and analysis

As seen in the Table eight, Measurement and Analysis lies in the initial stage in the case company. There were some security metrics in use, and they were well organized, defined and had a person assigned to look up on.

During the research period the need for an established security metrics was addressed multiple times by the middle management. Some important security related functions were measured, but the lack of decision making prevented establishing clear security metrics. The visibility of current metrics was feeble outside of the corporate security team. This explains why Measurement and Analysis stays around the level “Initial”.

Process and product quality assurance

There occurred dispersion in the interview results on, whether there are corporate security quality requirements and on who establishes them. It was clear that there were a few corporate security quality requirements. The requirements often were based on executed/not executed -principle.

Active security processes were mainly maintained by the security team and the quality assurance was decided by the acting person or security team. Though, this seemed to be a good practice when taking in to consideration the size of the security team and the number of different functions. Needless to say, quality requirements which are based on well-established metrics, serve better in the long run.

Supplier agreement management

Supplier agreement management was well organized in the company. There were named responsible persons which worked on their own field. The overall picture from security related document management seems to be blurry to the CSO which could be partly explained by the autonomous agreement management of the security team members. This culture was established in the case company already before the significance of corporate security became evident. During the research the author was not able to reach a process definition about supplier agreement management.

Work monitoring and control & Work planning

Not surprisingly, Work monitoring and control & Work planning were among the best graded process areas. This could be explained by their relation to the security team and its autonomous work. Work planning and monitoring were mostly performed within the security team which enabled a relatively smooth handling of procedures.

Judging by all the research methods, there were yearly plans made by the security team aiming to develop corporate security, the plans were discussed and accepted by certain instances and deviations from the plan were reacted with agreed measures. Work monitoring and controlling & Work planning were recognized as important elements by the employees.

6.3 Maturity level 3 process areas

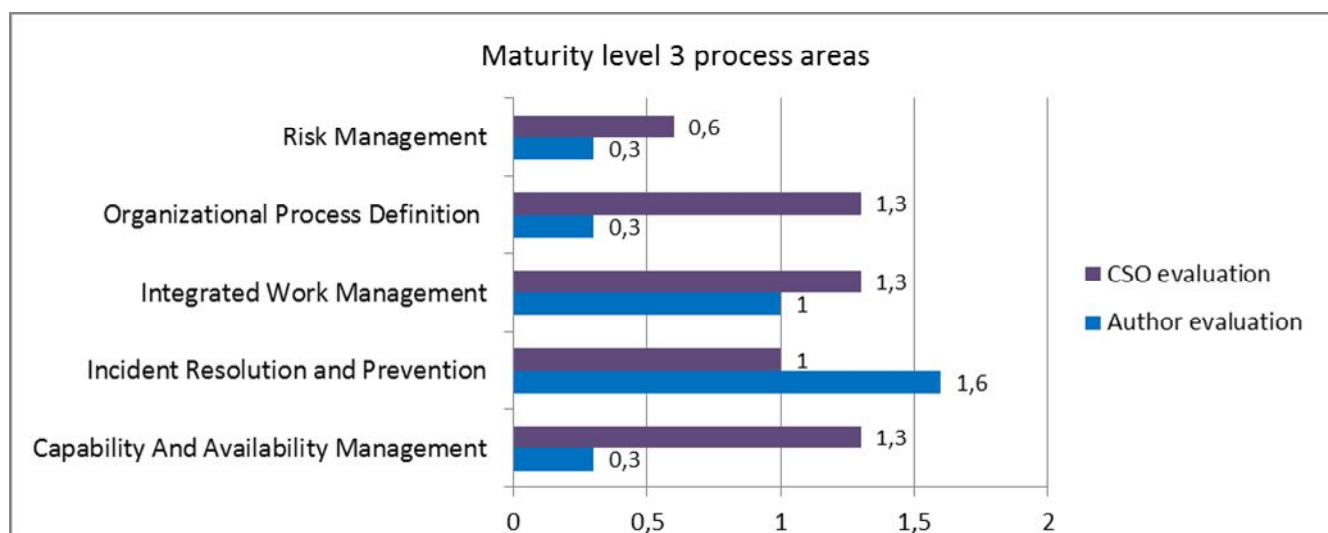


Table 9: Maturity level 3 process areas

Capability and Availability Management

The most striking difference between the author's and the CSO's view occurred in regards to Capability and Availability Management. The first described this process area as incomplete, whereas the latter had an overwhelmingly better picture on the function. The author's view

bases on the interview results which were rather obscure even though the availability of corporate security services was generally recognized by most of the participants.

Capability of corporate security was instead less recognized and occasionally linked to crisis scenarios. This is partly true, but does not respond to the recognition of the daily capability. One of the interviewee pondered if there was enough demand for corporate security and what would be its favorable level in order to provide for a permanent corporate security capability.

Incident resolution and prevention

This process area gave twofold results. On one hand, the case company had evolved in incident management. The handling of incidents shifted from an “ad hoc” case-handling in to a more consistent, organized and far seeing procedure. The development of security incident management was one of the first jobs of the author in the case company.

On the other hand, the process was not yet institutionalized, there was no responsible person appointed for the process, and some of the incidents were still dealt with in different instances. A definition of any incidents had not been drafted.

Integrated work management

There's no remarkable dispersion in the opinions on IWM. Corporate security is seen to be substantially integrated with all the other functions, even intertwined. The security team's normal tasks are not an obstacle for security matters, and vice versa.

Thus, the integration is not totally completed, e.g. the project organization and the security one are still functioning separately. Of course, the latter supports the business with incident handling, challenges and via training. The ultimate goal - a corporate security that affects through the linear organization - remains to be reached.

Organizational process definition

Defining processes is clearly unfinished. It's worth mentioning that the view of the author and the CSO differed a lot. The first described this process area as incomplete, whereas the latter had a seemingly better picture on Organizational Process Definition. One explanation can be found in the experiences of the two: the CSO was appointed during the research period and he had to familiarize himself with the process descriptions in use, whereas the trainee had a longer understanding on various procedures and descriptions.

In the broader picture, the corporate security core components have indeed been identified and established, but scaling from top to down for more detailed processes, the functions lack

an accurate description. The functions are working with routine and are based on verbal agreement. Then again, it is not a big problem, since the security organization is small, relatively new and personnel changes are not common.

Risk management

The lowest grades were given to Risk Management. It was also the most controversial topic considering the development of risk management in the case company. During the research a major risk analysis was conducted, and the author participated.

Risk Management was activated in the case company by the top management during the research period. The process was taken in use by the top management, which manifested itself during the risk assessment procedure. Since it was executed on a strategical level (and not on the everyday one), the assessed risks were high-level risks. Understandably, the lower level risks were not noticed, but as a consequence, the concerns of security team were more or less left aside.

The implementation of the risk management plans or intentions in lower levels remained unclear till the end of the research. Seemingly some of the top management interviewees considered it a good idea to direct risk management on certain support service areas. Decisions of analyzing risks within key business processes remained ambiguous to the author alike.

7 Development proposals

After 2013 no workshops has been held. Another security workshop could be a good event to summarize the development during the past years, and to decide the next goals to be achieved in the field of corporate security.

The case company has no comprehensive contingency plan. *Contingency plan* is a critical element during the time of crisis, and it enables faster and planned recovery for business operation. The case company had planned to have their first contingency plan ready during 2017. In order to have the contingency plan ready, the company must initiate risk measurements on its core business operations and key support services.

- The company's corporate security team should form a discussion platform between the corporate security team and the business elements in order to enforce implementation of security procedures inside the company and enhance the security culture in the company.
- Corporate security year clock
- List of documents, which must be updated periodically

The case company has created necessary guidelines to some of its operation areas. However, the deployment of the guidelines and responsibilities to managerial level employees has not been completed.

- Develop processes how to implement security practices to the employees.
- Produce a basic guide for management employees how to deal with security issues.

7.1 Responsibilities & Strategy

Responsibilities in the case company has been defined on the level of security policy, and the top management and security team are aware of their responsibilities. But based on the interviews and observation, the top management is only partially committed to develop corporate security. The top management's awareness of corporate security needs to be augmented, particularly on how to perceive, measure and execute corporate security. The security team hankers after a broader involvement from the top management and interest groups. Hence, the top management should define the objectives and metrics for corporate security based on the risk management and strategy; and then assign the objectives to the security team which in return will give the top management further input on what is the corporate security situation and how it is developing.

The case company's corporate security strategy is based on the effectual security policy and strategic level risk assessment which is a continuous process. The next step would be to create a strategy based on the risk assessments. Metrics should concern the most significant risks in order to monitor their evolution. A problem is that the top management has only one security related metrics in the top management metrics. The target goals of corporate security and how to achieve them should be considered. Those target goals could for example be:

- Valid contingency plan
- Information security aware personnel
- The target risk level of significant risks
- Implementing security management to the top and middle management
- Better understanding of the market situation
- Insuring competence in most significant projects

The top management should consider increasing its visibility in the security team. This could be done by having a member of the top management participating the security team meetings once or twice a year. The person could be rotated. This would enable the access to the firsthand information of corporate security, and on the other hand, the security team would get more direct contact with the top management, enabling a better decision making.

The case company should consider how to make employees more aware of their security responsibilities:

- Project risk management
- Escalating problem situation & incidents
- Reporting incidents

7.2 Risk management

Two major risk assessments were conducted in the case company during 2016. The first one was conducted to map out risks in four core areas: Operative, Strategic, Economic and Damage risk areas. The second risk assessment was conducted to one of the core business areas of the company, and it didn't provide much additional information. Later on, the risk management process was assigned to a work group. It remains to be seen how this arrangement will function.

First risk assessment was conducted on higher levels and concerned rather strategic risks. The risk assessment should be conducted step by step in lower levels, as the second risk assessment was performed. Though it didn't generate much additional information, the cascading should be carried on. Defining the critical processes and conducting the risk assessment to them should be the next step.

The aspect of risk assessment enabling the taking of managed risks should be considered in the case company. The idea is that the risk assessment brings up likely risks of new possibilities; this would enable the preparations and control of the risk before utilizing the risks.

7.3 Contingency plan

Critical processes of the core business operations and key support services need to be defined. These processes could be described as indispensable for the success of the business operations.

The following factors could be included:

- Recognizing markets
- Success in sales
- Project work
- Personnel and coping at work
- Work spaces and equipment
- Information management

Contingency plan which takes in to account the risks of critical processes with major negative impact to the company's business operations should be established. The risks which have high magnitude effect should all be considered in the contingency plan. Risks which have high frequency, but low magnitude, are not as necessary to be included in the contingency plan, but rather require actions to lower the frequency rate.

The plan should include the most critical factors. Those factors could be:

- How long the company's economy can stand the complete halt of business operations
- Spare workspaces
- Spare equipment
- Information connections
- Recovery of information
- Working capability and repositioning of personnel

These measures should be conducted at least to a certain minimum preparedness level. There is a clear chain of communication and initiation of proper procedures in case of a significant risk realizes. It's not inevitable that all the critical operating processes have risks which have significant magnitude to the company's operations. A decision should be made which risks could potentially cause a severe business operation interruption and should be prepared to with a contingency plan. On the final stage of contingency plan the procedures should be rehearse.

7.4 Metrics & Monitoring

The case company is in a state, where clear corporate security metrics are not achieved, and the ones which are being measured, are not forming in to clear processes. The problem in the situation seems to be the expectations between the top management and the security team. The latter awaits the top management to express what they want to be measured, whereas the first seems to expect ready metrics and information of the key measurable factors to be handed out.

The only official security meter of the top management is sick leaves. The resources which are used to security are also monitored to some extent. This measurement is preferable with set targets and with a scale whether or not those targets are achieved. The company has executed a security plan annually since 2014, and it is accepted by the Support Services Management Team, but the responsibility for the plan has been left to the CSO and the security team. The security team should implement a security year clock to enhance its efficiency. It would offer the top management a tool to better follow the performed security work.

The top management should increase security managerial point of view: the corporate security and the continuity perspective should be taken account in decision making. Also, the goals of security management and metrics should be created. These metrics could be:

- Most significant incidents
- The costs and interruption caused by incidents
- The decisions and actions of the security team
- Internal security trainings and the participant count
- Corporate security support requests
- Customers' preconditions for the case company's corporate security
- Follow-up of the corporate security development and resources

7.5 Incidents management

Corporate security incidents have been processed on individual level, in the security team, the Support Service Management Team and the top management. When incidents are managed on multiple levels, the information of incidents is harder to deal with, and it doesn't necessary reach the responsible personnel. Without proper management, the incident management suffers from delays, missing of conclusions or forgetting of the incidents.

Incident management records give valuable information from the state of the company's corporate security threats and vulnerabilities, which further on help the company to direct measures. The recognition of information collected from incidents and its analysis require development of a better information management. Appointing responsible person(s) to manage the procedure should be considered.

The security team has a proposal of the incident management procedure marking the managerial responsibility for the security team. The team determines the responsible entity to handle an individual incident. This proposal and management procedure is already in use, but requires recognition and validation. Later on, the incident management procedure should include the roles of key interest groups, such as customers, employees, higher management and partners.

The escalation of incidents to higher management levels requires development:

- Appoint person to be responsible for corporate security incident management
- Implementing severity scale of incidents which includes escalation points. These could be tied to the costs, time, interest group or theme
- Define type of incidents which require escalation
- Agree with higher management levels of which incidents they want to be acknowledged

- Defining the difference between security incident and quality incident
- Every employee to recognize incidents on normal work and how to report and escalate
- Agreement on incident management responsibilities, roles and escalating should be established and deployed to interest groups

7.6 Implementation of security activities

Implementation of security activities in the case company happens through the security team, sometimes including a consultation of the top management. The security team and the top management should agree on the implementation of security activities. For example: Corporate security team proposal to the top management => Review and comments of the top management => Corporate security team modification => Modified proposals => Accept/reject => Orientation of corporate security team, CSO, departments and other interest groups.

Development objectives of implementation of security procedures:

- A process of gathering and changing information between the security team and business should be established. The current information sources should be identified, e.g. every employee, project manager, e-mail, hearsay or other ways of communication. Popular information channels should be recognized, the main information collection channels should be chosen and informed to the users to simplify the gathering process. However, receiving information from other sources has to be possible, but still the recording of information must be guaranteed.
- Agree on how the security processes are implemented to the operations of the case company. (Acceptation, orientation, use and continuous development)
- Security instructions of the middle management. A manual which would include main sections of corporate security and a harmonized description of procedures. Also, the most important factors and subjects required by the most relative interest groups. The guide could include instructions of security procedures and services which are available for employees. The manual could be included in the quality handbook.
- Promote corporate security in a positive manner. Corporate security is a supportive function and the purpose is to help employees. The aim is to make employees more aware of, it and willing to contact the security team, in case of uncertainty or incidents. The image of penalty and extra work when contacting security should be reduced to minimum.

7.7 Reflections

The case company offered an information rich and a challenging environment. The company was large enough for various phenomena to study and multiple components to develop. The used research methods served well the purpose of the thesis. Information from some key functions could have added nuances to the thesis.

The Capability Maturity Model Integration offered an inspiring and challenging platform to evaluate corporate security service. The process areas were thoroughly described, and they gave suitable frames for the evaluation. The Generic and specific goals of process areas were a precise measurement tool. The evaluation of the original model was too strict, so the evaluation system was loosened, and the generic practices were accentuated. In the results the table of generic goal evaluation is present, but the evaluation of specific goals is absent. The specific goals goes in detailed level how a process area should be run. Considering the state of corporate security in the company, a deeper analysis of specific goals would have been premature and unfair, since the model was implemented for the first time.

Visibility of the top management decision making and project work could have been more comprehensive. The actions that the top management execute have an impact to corporate security and the security team. A better vision to the top management could have offered information from commitment, situation awareness and communications of the top management to the organization and security team. The basic business operation of the case company is project work. A deeper perception of project work could have given a more comprehensive understanding of the security needs and defects in the everyday work.

Corporate security development is a complicated research object. When handling security as a supportive activity, instead of the main product the approach changes. When security is the wanted goal it's acceptable to do whatever it takes to achieve the wanted objective. While having security as a supportive factor the resources are allocated according to the requirements of accomplishing the main objective. Understanding this contributes for a healthier partnership between security and business.

7.8 Thesis evaluation by the thesis supervisor in the case company

Choosing thesis topic, aim of the thesis

Case company has a clear need to develop corporate security further from its current state, the thesis clearly responses to this need. Kalle has been integral part of company's safety & security team during internship, gaining clear view for current state of corporate security and development issues. Furthermore, Kalle has shown to be able to work in changing environment due to personnel changes during internship.

Theoretical framework

The field where case company operates gives some limitations to source material. The field has not been researched in large scale and therefore the amount of publications is limited. Chosen CMMI is applicable for case company operations.

Methods, thesis process, ethical issues, reliability

The methods used in thesis process are described in thesis. Written descriptions and actual methods are in line with each other. Chosen methods are applicable for thesis process keeping in mind the thesis limitations - thesis considers safety & security services leaving safety work at production off from thesis. Co-working with company thesis supervisor has been constant, but in a productive way, Kalle has worked independently during actual thesis writing process. During the end of internship, the current state of thesis and findings were communicated to larger audience.

Results and recommendations

The results of the thesis are what were expected. From the thesis, key findings can be directly converted to development projects, and analysis of interviews gives good background information about the ways safety and security should be developed in future.

Presentation, written form of the Thesis

As a result from the problems outlined in theoretical framework-section, chapters introducing the reader to CMMI-model seem to be a bit out from the scope of work at first sight. Issue is dealt with later on, which leaves no open questions. Overall, the form and language used in thesis is clear and punctual.

References

Printed sources:

Baszanger, I. & Dodier, N. 1998. Ethnography Relating the Part to the Whole. In Silverman (ed.) Qualitative Research. 2nd edition London: Sage Publications, 8-23

Brinkmann, S. & Kvale, S. 2015. Interviews Learning the Craft of Qualitative Research Interviewing. Los Angeles: Sage Publications.

Cabric, M. 2015. Corporate Security Management Challenges, Risks and Strategies. Oxford: Butterworth-Heinemann.

Eskola, J. & Suoranta, J. 1998. Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino.

Heljaste, J-M. Korkiamäki, J. Laukkala, H. Mustonen, J. Peltonen, J. & Vesterinen, P. 2008. Yrityksen turvallisuusopas. Helsinki: Helsingin seudun kauppakamari.

Kananen, J. 2013. Design Research (Applied Action Research) as Thesis Research. Jyväskylä: JAMK University of Applied Sciences.

Kovacich, G. & Halibozek, E. 2003. The Manager's Handbook For Corporate Security Massachusetts: Butterworth-Heinemann.

Leppänen, J. 2006. Yritysturvallisuus käytännössä - turvallisuusjohtamisen portfolio. Helsinki: Talentum.

Marshall, C. & Rossman, G. 2011. Designing Qualitative Research Fifth Edition. California. Sage Publications.

Miller, J. & Glassner, B. 1998. The 'Inside' and the 'Outside' Finding Realities in Interviews. In Silverman (ed.) Qualitative Research. 2nd edition. London: Sage Publications, 99-112

Electronic sources:

Business dictionary. 2016. Dictionary: Defines development. Accessed 20 September 2016.
<http://www.businessdictionary.com/definition/development.html>

Capability Maturity Model Integration. 2010. CMMI for Services, Version 1.3. Accessed 31 October 2016.
<http://www.sei.cmu.edu/reports/10tr034.pdf>

Dictionary Cambridge. 2016. Dictionary: Defines development. Accessed 20 September 2016.
<http://dictionary.cambridge.org/dictionary/english/development>

Elinkeinoelämä. 2017. Mitä teemme? Accessed 5 January 2017
<https://ek.fi/mita-teemme/>

Elinkeinoelämä. 2016. Elinkeinoelämän yritysturvallisuus-malli. Accessed 28 October 2016.
http://ek.fi/wp-content/uploads/yritysturvallisuus_2016.pdf

What is Capability Maturity Model? (CMM). Accessed 11 November 2016.
<http://www.selectbs.com/process-maturity/what-is-the-capability-maturity-model>

What is Capability Maturity Model Integration? (CMMI). Accessed 11 November 2016.
<http://www.selectbs.com/process-maturity/what-is-capability-maturity-model-integration>

Private interviews:

Anonymous A. Case company. Interview with the author. 17 October 2016. Helsinki region.
Personal communication.

Anonymous B. Case company. Interview with the author. 17 October 2016. Helsinki region.
Personal communication.

Anonymous C. Case company. Interview with the author. 17 October 2016. Helsinki region.
Personal communication.

Anonymous D. Case company. Interview with the author. 18 October 2016 Helsinki region.
Personal communication.

Anonymous E. Case company. Interview with the author. 19 October 2016. Helsinki region.
Personal communication.

Anonymous F. Case company. Interview with the author. 19 October 2016. Helsinki region.
Personal communication.

Anonymous G. Case company. Interview with the author. 21 October 2016. Helsinki region.
Personal communication.

Anonymous H. Case company. Interview with the author. 21 October 2016. Helsinki region.
Personal communication.

Anonymous I. Case company. Interview with the author. 21 October 2016. Helsinki region.
Personal communication.

Anonymous J. Case company. Interview with the author. 24 October 2016. Helsinki region.
Personal communication.

Anonymous K. Case company. Interview with the author. 24 October 2016. Helsinki region.
Personal communication.

Anonymous L. Case company. Interview with the author. 26 October 2016. Helsinki region.
Personal communication.

Figures

Figure 1: The Finnish Confederation of Finnish Industries corporate security model.....	10
Figure 2: Shiva's circle of constructivist inquiry (Marshall & Rossman 2011, cited in Crabtree and Miller 1992, 60)	15
Figure 3: CMMI - three critical dimensions (CMMI for services 2010, 4).....	21
Figure 4: Illustration of the CMMI components (CMMI for services 2010, 10)	22
Figure 5 : Continuous & Staged Representation (CMMI for services 2010, 22)	24
Figure 6: Continuous & Staged preview (CMMI for service, 2010, 32)	29

Tables

Table 1: Material used in document analysis.....	20
Table 2: Process areas (CMMI for services 2010, 33-34)	23
Table 3: Comparison of Capability and Maturity levels (CMMI for services 2010, 22)	25
Table 4: Generic Goals & Practices (CMMI for service, 2010, 57).....	30
Table 5: Educational background of interviewees.....	34
Table 6: What is corporate security?	35
Table 7: Responsible for security	36
Table 8: Maturity level 2 process areas	44
Table 9: Maturity level 3 process areas	45

Appendices

Appendix 1: Interview Questions	61
Appendix 2: Observation results.....	62
Appendix 3: Summary of interview results of process area questions	67
Appendix 4: Capability & Maturity evaluation of the author and CSO	72

Appendix 1: Interview Questions

General questions

1. What is your position?
2. Could you tell about your education & work background and if you have worked before with security?
3. How long have you been working for the company?
4. How would you define corporate security?
5. Who is responsible for corporate security in the company?
6. How corporate security appears in business?

Measurement and Analysis

1. How corporate security is measured in the company?

Process and Product Quality Assurance

2. Does corporate security have quality demands? How is their fulfillment ensured?

Supplier Agreement Management

3. How are the company's security related agreements administered?

Work Monitoring and Control

4. How corporate security and its development related work is supervised and how it is controlled in the company?

Work Planning

5. How would you describe the corporate security work planning in the company?

Capability and Availability Management

6. What is the capability and availability of corporate security in the company? Does it have a strategy?

Incident Resolution and Prevention

7. How are the corporate security incidents and the prevention of the incidents managed in the company?

Integrated Work Management

8. How is the integration of corporate security work to other work taken in to account in the company?

Organizational Process Definition

9. Have the corporate security processes of the company been described, if they are what kind of issues has been taken in to account in the descriptions?

Risk Management

10. How is risk management operated from the perspective of corporate security in the company?

Appendix 2: Observation results

Entry headline	Content	Highlights
Risk analysis seminar (1/3) II/2016	<ul style="list-style-type: none"> • Strategic risks • Economical risks 	<ul style="list-style-type: none"> - Top management, security team & industry sectors were well represented - Advantages & disadvantages of personnel - Information security risks & risk mitigation - The company has good reputation - Wanted partner to co-operation projects with rival companies - Information systems were debated - Competition is hard - Open discussion
Meeting with the CSO II/2016	<ul style="list-style-type: none"> • Time concerns • Communication 	<ul style="list-style-type: none"> - The CSO's time is going to own project work and security work is suffering - The company had decided on major investments without communicating with the CSO
Security team meeting II/2016	<ul style="list-style-type: none"> • Risk analysis seminar • Information security • Security management & communication • Crisis communications • Occupational health and safety 	<ul style="list-style-type: none"> - Discussion on information security vulnerabilities & culture, controversy between information services and employees on information security - Organizing occupational health and safety in the company.
Meeting with the CSO II/2016	<ul style="list-style-type: none"> • Risk analysis seminar • Occupational health and safety 	<ul style="list-style-type: none"> - Role ambiguity on occupational health and safety issues due to a labor safety inspection.
Support services management team meeting III/2016	<ul style="list-style-type: none"> • Discussion on current issues 	<ul style="list-style-type: none"> - Discussion on crisis communications possibilities - Information security issues - SSMT decided to start monitor one physical security meter
Meeting with the CSO III/2016	<ul style="list-style-type: none"> • Security management matters 	<ul style="list-style-type: none"> - Changes to the security team coming from top to down - CSO has no development discussion on security management duties - Question to CSO: "Is security working by itself already?" - According to CSO, Chief Information Officer (CIO) has not enough time for security issues
Risk analysis seminar (2/3) III/2016	<ul style="list-style-type: none"> • Operative risks • Damage risks 	<ul style="list-style-type: none"> - Top management well presented, though CEO and quality manager left during the seminar

		<ul style="list-style-type: none"> - CSO brought up resource deficit on security management - Conversation was good & open
Meeting with industry segment representatives III/2016	<ul style="list-style-type: none"> • Security matters in particular industry field • This industry field has more and severe risks 	<ul style="list-style-type: none"> - The industry field has clear security procedures - These procedures are working inside the industry but do not appear at the security management of the whole organization.
Meeting with the CSO III/2016	<ul style="list-style-type: none"> • Risk analysis seminar • Security management matters 	<ul style="list-style-type: none"> - Discussion on risk analysis seminar - The top management has substitute arrangements but the security team is not aware of them - CIO is very busy limiting the time for security issues
Meeting with the CSO III/2016	<ul style="list-style-type: none"> • Support service info • Last year's security plan • Security managerial matters 	<ul style="list-style-type: none"> - Planning the matters to present at the support service info - Check over & tracking on last year's security plan - One industry segment had requested help with security issues from the CSO on January. It was brought up now.
Meeting with industry representatives III/2016	<ul style="list-style-type: none"> • Project work • Security management 	<ul style="list-style-type: none"> - At basic work there are security demands from the customer and case company
Risk analysis seminar (3/3) III/2016	<ul style="list-style-type: none"> • Revision of previous seminars and summary 	<ul style="list-style-type: none"> - Variability of the involved personnel was kept as a good factor - The case company has responsibility over subcontractors' work - Demand for the risk analysis was recognized and will be taken to regular use by the top management - It-security woke discussion, on the other hand there was faith for self-performance, but also the magnitude of possible incidence was addressed -No stands were taken to the incident response capability
Risk analysis seminar III/2016	<ul style="list-style-type: none"> • Comments of the seminar hosts (No case company representatives present) 	<p>Positive:</p> <ul style="list-style-type: none"> - Well preformed, one of the best - Open and willing to develop - Strong opinion of the CEO - Risk analysis tool was taken in real use and not as a standard procedure - Issues were dared to bring up and

		<p>the top management was challenged</p> <p>Negative:</p> <ul style="list-style-type: none"> - Big amount of participants caused some passiveness - Emphasis of certain areas influenced the whole risk analysis e.g. security issues
<p>Security team meeting IV/2016</p>	<ul style="list-style-type: none"> • Discussion on risk seminar • CSO changing employer • New communication manager present 	<ul style="list-style-type: none"> - Common opinion was that the risk seminars were scratch of surface - Top management had reviewed and modified the results of the risk seminar - CIO noted that risks are recognized, but resources are not sufficient and important decisions are not advancing especially related to contingency planning - Communications problems were defined in the flow of information - Top management had decided that no fulltime CSO will be appointed
<p>Meeting with the CSO IV/2016</p>	<ul style="list-style-type: none"> • CSO changing employer • Risk seminar results 	<ul style="list-style-type: none"> - No meetings with the CEO were held during last six months - Security co-operation with different industries has had difficulties - CSO and the top management differed in their ideas decisively - Top management had decided following: <ul style="list-style-type: none"> * Risk management may be used in big projects * Risk management is included to top managements year clock & if necessary risk management will be continuous process * The finance manager will be in charge of the risk management process
<p>Intranet announcement IV/2016</p>	<ul style="list-style-type: none"> • CSO open recruitment 	<ul style="list-style-type: none"> - In addition to normal duties - Responsibilities of the CSO - Development tasks for 2016 - Task requirements
<p>E-mail exchange with CIO V/2016</p>	<ul style="list-style-type: none"> • Proposal for developing contingency plan 	<ul style="list-style-type: none"> - Proposal to assist develop contingency plan - Proposal rejected due to strategy update and internal processing

		<ul style="list-style-type: none"> - A stand will be taken to contingency plan after strategy update is complete
Meeting with CEO V/2016	<ul style="list-style-type: none"> • New CSO • Information security auditor competence acquired 	<ul style="list-style-type: none"> - Four CSO candidates inside the company - Information security auditor competence was acquired to certain industry area, this has had improving impact to the overall security of projects - Promised security audition in future
Email Overview VI/2016	<ul style="list-style-type: none"> • Information security incident • Information security support request 	<ul style="list-style-type: none"> - Information security incident was reported and the management of the incident was unclear - CIO shared a help request to a project offer with tight schedule
Intranet announcement VI/2016	<ul style="list-style-type: none"> • Experienced new CSO appointed 	<ul style="list-style-type: none"> - Responsibilities of CSO - Occupational health & safety manager tasks - Development of corporate security
Security team meeting VI/2016	<ul style="list-style-type: none"> • New CSO present • Pragmatic approach to corporate security development 	<ul style="list-style-type: none"> - CSO presented himself - He required time until august to orientate - No big decisions were made
CEO schedule VIII/2016	<ul style="list-style-type: none"> • Noticed from CEO's schedule 	<ul style="list-style-type: none"> - Training for challenging situation in project work marked in his schedule - No other information available
Security team meeting IX/2016	<ul style="list-style-type: none"> • Security incidents • Crisis communication guidelines • Thesis review • Information security training program offer 	<ul style="list-style-type: none"> - Nine security incidents were reviewed and processed - Top management had requested a crisis communication guidelines - Information security training program was reviewed and decided to acquire one
Security team / The CSO XI/2016	<ul style="list-style-type: none"> • On-going development • Security incidents • Information security training program • Document classification • Incident management process 	<ul style="list-style-type: none"> - Responsibilities were appointed on development projects - New CSO up to date with corporate security management - Incident processing was inadequate compared to the maturity model requirements - New information security process was planned to be taken in use * Lack of unambiguous procedure within implementation

		<ul style="list-style-type: none"> - Draft of documentation classification was decided to be done - Next year's (2017) security plan was not reviewed *It remains to be seen how it will be managed - Incident management process was not reviewed
The CSO XI/2016	<ul style="list-style-type: none"> • Information security training program presentation event • Retrospect of the current security plan (2016) • Review of separately retained documents 	<ul style="list-style-type: none"> - Common opinion about the information security training program was that it meets the requirements - Implementation and supervision of the security plan are heavily dependent on the CSO - The trainee had personally preserved security related documents which were then shared * The documentation procedure of security documents was insufficient
Overall review XII/2016	<ul style="list-style-type: none"> • Internship nearing the end, successor has been selected • Thesis results • Upcoming challenges & further development needs 	<ul style="list-style-type: none"> - The successor is from one of the industries and continues the work in addition to his normal duties - First results of thesis are emerging - The company has will, but a vague understanding of the overall corporate security - Upcoming challenges include the integration of corporate security to the company's operating culture, continuation and implementation of risk management procedures and development of contingency plan - The CSO finds work challenging with the allocated resources

Appendix 3: Summary of interview results of process area questions

Measurement and Analysis

It is evident that the case company has corporate security metrics in use. The use of the metrics on the other hand is not clear. Measurement is taking place on different organization levels, and the corporate security metrics are not commonly agreed. Some of the interviewees seem to have a clearer picture that measurements are taking place, but lack the confirmation if the measurement really happens, or if the metrics are defined. The current security metrics that were detected during the research were mainly defined by the security team, but it came evident that the top management also has its own security related metrics.

The metrics has been mainly based on a scale executed/not executed. The tracking of the metrics is a responsibility of the metrics owner. This means that the accountable person manages the metrics and information from the metrics is mainly, if not only, shared by the same person.

The tracking of security metrics and reporting the results has no sophisticated pattern and there is no established process to analyse the metrics. Communication about the information acquired from the metrics is not established. There is also clear dispersion between employees working in business and support services. Those who do not work regularly with security issues have less information about security metrics.

Process and product quality assurance

There is a dispersion on corporate security quality requirements and on how they are executed. Some of the interviewees say that there are requirements, while others say that there are no quality requirements or the requirements are not pointed out or set to be tracked by the responsible person, excluding the security plan. The whole management of corporate security seems to be a bit unclear to some of the interviewees. Then again, corporate security work has been divided to different sections and the main responsibility of a particular section is assigned to the responsible employee. There was a clear dispersion on how different sections had managed the quality assurance.

The security work has qualitative requirements, and the principle is that the requirements are filled or unfilled. Legislation sets some corporate security standards to be fulfilled. The CSO seemed to have the main role to set the corporate security quality requirements to some extent. Also, the customers could set corporate security quality demands, and these demands were managed either on project work level or in the top management depending on the task.

Supplier agreement management

Supplier agreement management seems to have well-established processes, and the responsibilities have been divided clearly. The personnel are well aware how the responsibilities are divided and how the supplier agreement process works. The supplier agreement management had no clear process description.

Work Monitoring and Control

A yearly corporate security plan is conducted. The plan is accepted by the support service management team and CEO, and it is being supervised by the CSO. There was a considerable unawareness about the security plan among the interviewees. Control of the actual corporate security work was done in the security team. However, the top management followed the work of the security team and allocated resources. The security management work was felt to miss certain firmness to get tasks completed by some of the interviewees.

It was pointed out that some of the projects had a stricter security control, and expected the control to be on a higher level. Reacting to deviations from security plan relied on the CSO. Corporate security development was seen as a general jargon by the common employees.

Work Planning

The security team members had a better overall picture about the work planning, than interviewees who worked in business. The settled working practice in the security team was first to handle acute issues, then current concerns and finally development projects. Some deprivation occurred about the corporate security strategy.

Some viewed the security plan as a strategy, and others were opting for a longer period plan. Some of the security team members perform independent security planning within their responsibilities area.

The top management has also made decisions which have affected to the work planning of the security team. The planning and clarifying the targets of project of the security team are seen somewhat incomplete. Risk-based planning came up as a possible method for work planning.

Capability And Availability Management

The capability and availability of the corporate security are not defined. The CSO works in addition to his normal duties. Time is granted if there are acute issues, but otherwise the CSO has allocated resources to corporate security. Common opinion was that the standard processes were running well, and that the system would be measured in time of crisis. The discussion generally went to crisis situations and to the question whether the resources would be

adequate then. There is no written strategy, but some initial agreement has been made. There was some confusion about the yearly security plan's relation to the whole security strategy.

The capability and availability were seen to be on sufficient level, but the usage and increasing awareness of the possibilities for common employees could be improved. The security team is capable to produce material, but the capability to make it available is another thing. There was some wondering amongst the interviewees whether it is necessary to develop the capability management of corporate security. One brought up the question of demand, if there is such for corporate security and what is the volume and how to keep the volume at a sufficient level. The period without CSO is mentioned as a clear factor which had lowered the capability of corporate security function. The question whether the business utilizes the supportive function enough, was raised alike.

Incident Resolution and Prevention

Incident reports are few and many of them come through unofficial channels, though there was an official channel in use. Usually incidents were solved already before the official procedure in the security team. The practice in case of incidents has been an imminent response due to the urgency, and the handling of incident was left to the next security team meeting. Since the security team consists of only few members, the need for an incident procedure definition was scant.

There were no official criteria for incidents. The description of any incident was missing. Another thing is the project incidents which have their own procedures and include other than security incidents e.g. quality assurance incidents. A remarkable notification was that there are incidents that never reached the awareness of the CSO or of which he was informed long after.

Integrated Work Management

The corporate security work was seen to be very integrated to the organization. The CSO's main work is on business, and the rest of the security team has natural roles in the supportive services. Each of these has security duties in addition of their daily job. The security tasks integrate well to the normal tasks of the security team members. The current operating model is considered fine.

In the beginning project management lived its own life, and security procedures were forming according to the needs that occurred. The project organization and the security organization have been kept apart, the aim is that corporate security would affect through the line organization. It was mentioned that there is no separate security function and the corporate securi-

ty is interleaved in the organization. The corporate security has supported business with incidents, challenges and through training. Still, the implementation work to fully support the business is unfinished.

Security is seen as a part of daily processes. One interviewee pointed out that security should not be done just for security. One opinion was that a requirement for a fulltime Chief Security Officer should be based on the needs of the business.

Organizational Process Definition

Security management and the organization are well described. Some security procedures has been described, and a corporate security management system was being planned to be taken in use. The system had processes described from above, but the content wasn't necessarily ready. The idea was to get primer from a management system standard which was being acquired at the time. In general, relatively few processes have been described, and the work has been purposely left undone, though the existence of some processes are communicated. The work of defining processes was depicted as incomplete.

There was some hesitation on the knowledge whether there are process descriptions available. One interviewee did not identify process definition at all. An interviewee representing business considered the understanding of security processes irrelevant, but acknowledging the procedures important. A relatively short informative guideline was preferred to a hundred page one, pointing out the wish to have relevant information instead of jargon. There was no knowledge of a guideline directed to project managers.

On behalf of information security, there is a description on how to proceed with various projects. Some of the information security procedures are executed according to the will of customer.

Risk Management

The company has a risk management tool in use which was implemented during 2016. It is reviewed twice a year in the top management. Still, the risks are managed in multiple locations in the company, though many project risks are not directly connected to the corporate security. Previously, the risk management was less organized and it was mainly, on the responsibility of the CSO and the security team. Some risk assessment has been executed in the support services. Since the new tool the risk management has been developing, and the next step is to deploy the risk management process down in the organization. The security team and the supportive service were seen as a favorable way to slightly expand the risk assessment process.

Some measures of crisis preparedness were executed. The company needs to create a contingency plan. Risk mitigation plans and actions have been planned to the most known, biggest and important risks. The next phase is to execute the plans and actions. One of the business representatives had an unsound picture of the current state of risk management.

Additional question asking for comments

The interview questions were felt hard, but good. A wish was to have more determined cooperation with the top management about goals and strategy to understand the produce of additional value through corporate security. Clear security metrics with enough high level tracking and continuity were wished at least on yearly basis, so that trends could be spotted.

Lack of resources, the inefficient deployment and need for resources were brought up. Interviewees with diverse experiences felt that on long-term the development has had an upward trend.

Appendix 4: Capability & Maturity evaluation of the author and CSO

Generic Goals and Generic Practice Evaluation

Process area	Author	GG1	GG2	GG3	CSO	GG1	GG2	GG3
Measurement and Analysis	1	0/1/0	3/4/3	0/2/0	1,3	1/0/0	4/5/1	0/1/1
Process and Product Quality Assurance	0,7	0/1/0	4/4/2	0/1/1	1,3	1/0/0	4/5/1	0/2/0
Supplier Agreement Management	1,6	1/0/0	6/4/0	0/1/1	1	0/1/0	0/9/1	0/2/0
Work Monitoring and Control	1,6	1/0/0	8/2/0	0/1/1	1,3	1/0/0	3/6/1	1/1/0
Work Planning	1,6	1/0/0	7/3/0	1/1/0	1,3	1/0/0	3/6/1	0/2/0
Capability And Availability Management	0,3	0/1/0	2/6/2	0/0/2	1,3	1/0/0	3/6/1	0/2/0
Incident Resolution and Prevention	1,6	1/0/0	5/5/0	1/1/0	1	1/0/0	0/9/1	0/0/2
Integrated Work Management	1	1/0/0	4/5/1	0/0/2	1,3	1/0/0	1/8/1	0/2/0
Organizational Process Definition	0,3	0/1/0	0/4/6	0/0/2	1,3	1/0/0	2/7/1	0/2/0
Risk Management	0,3	0/1/0	2/4/4	0/0/2	0,6	1/0/0	0/6/4	0/0/2

Specific Goals and Specific Practice Evaluation

Process area	Author	SG1	SG2	SG3	CSO	SG1	SG2	SG3
Maturity level 2 process areas								
Measurement and Analysis	1	0/2/2	2/2/0		1	1/2/1	1/3/0	
Process and Product Quality Assurance	0,5	0/2/0	0/0/2		2	2/0/0	2/0/0	
Supplier Agreement Management	1,5	1/1/1	3/0/0		1	0/3/0	1/2/0	
Work Monitoring and Control	1	3/4/0	0/3/0		1,5	4/3/0	1/2/0	
Work Planning	1,3	2/3/0	4/2/1	1/2/0	1	1/2/2	3/4/0	0/2/1
Maturity level 3 process areas								
Capability And Availability Management	0,5	0/2/1	0/0/3		1,5	1/1/1	2/0/0	
Incident Resolution and Prevention	2	2/0/0	4/1/0	3/0/0	2	2/0/0	4/1/0	2/1/0
Integrated Work Management	1,5	3/4/0	2/1/0		2	4/3/0	2/1/0	
Organizational Process Definition	0	0/4/3			1	2/4/1		
Risk Management	0,3	0/2/1	0/2/0	0/0/2	0,7	1/2/0	0/1/1	0/1/1