



TAMPEREEN TEKNILLINEN YLIOPISTO  
TAMPERE UNIVERSITY OF TECHNOLOGY

PEKKA LEHIKAINEN  
CUSTOMER RELATIONSHIP MANAGEMENT ENVIRONMENT  
FEATURES AGAINST INFORMATION SECURITY IN A CASE  
ORGANIZATION

Master of Science thesis

Examiner: Professor Samuli Pekkola  
and University teacher Ilona Ilvonen  
Examiner and topic approved at the  
Faculty of Business and Build Envi-  
ronment Council meeting on the 30<sup>th</sup>  
of October 2017.

## ABSTRACT

**PEKKA LEHIKONEN:** Customer relationship management environment features against information security in a case organization.

Tampere University of Technology

Master of Science Thesis, 63 pages, 7 Appendix pages

November 2017

Master's Degree Programme in Information and Knowledge Management

Major: Process and Product Information Management

Examiner: Professor Samuli Pekkola and University Teacher Ilona Ilvonen

Keywords: Knowledge Management, Customer Relationship Management, Risk Management, Information Security

Customer Relationship Management (CRM) is in many organizations a developing process, which is usually also integrated to the related information systems. Effective CRM and utilization of related information and data offers various benefits but there are also several challenges and risks related to the CRM from information security point of view. This research studies CRM environment and its features in a case organization from information security point of view.

Study was made in case organization with multiple interviews with the representative personnel. Material from the interviews was then analyzed and the discovered findings were evaluated with a risk analysis method described in the study. The results are being introduced and the most crucial findings are being highlighted and discussed more thoroughly. There was also an analysis made of these results, which is covered in this study too. In the end conclusion of the study is being introduced along with discussion of the reliability of the study and potential future researches.

Study shows that there were 15 challenges or considerations identified in the case organization CRM environment from information security point of view. Five of them were estimated to be the most crucial ones with the used framework. There are some resemblances found from the literature in comparison to the study findings. However, the results reflect mainly the situation in the case organization that can be used as a reference point when assessing other similar kind of situations.

## TIIVISTELMÄ

**PEKKA LEHIKONEN:** Asiakkuudenhallinnan tietoturvallisuuden piirteet esimerkkiorganisaatiossa

Tampereen teknillinen yliopisto

Diplomityö, 63 sivua, 7 liitesivua

Marraskuu 2017

Tietojohdamisen diplomi-insinöörin tutkinto-ohjelma

Pääaine: Prosessi- ja tuotetiedon hallinta

Tarkastaja: professori Samuli Pekkola ja yliopisto-opettaja Ilona Ilvonen

Avainsanat: Tietojohdaminen, Asiakkuudenhallinta, Riskienhallinta, Tietoturva

Asiakkuudenhallinta on monissa organisaatioissa kehityksen alla oleva toiminto, joka on usein myös tiukasti sidottu vastaaviin tietojärjestelmiin. Tehokas asiakkuudenhallinta ja siihen liittyvän tiedon ja datan hallinnan avulla on saatavilla useita hyötyjä mutta siihen liittyy myös merkittäviä haasteita ja riskejä tietoturvallisuuden näkökulmasta. Tämä tutkimus käsittelee asiakkuudenhallinnan ympäristöä ja sen ominaisuuksia esimerkkiorganisaatiossa tietoturvallisuuden näkökulmasta.

Tutkimus suoritettiin esimerkkiorganisaatiossa haastattelemalla useita aiheen kanssa tekemisissä olevia organisaation työntekijöitä. Haastattelujen materiaali analysoitiin ja tehdyt löydökset arvioitiin tutkimuksessa käytetyn riskienhallinnan arviointiin tarkoitettun viitekehyksen mukaisesti. Haastatteluiden pohjalta tehdyt tulokset esitellään ja tärkeimmät löydökset käydään läpi vielä tarkemmin. Tutkimuksessa käydään läpi myös analyysiä, joita tehtiin löydetyistä tuloksista. Lopuksi esitellään päätelmät tutkimuksesta sekä arvioidaan sen luotettavuutta ja mahdollisten tutkimuksen kohteita tulevaisuudessa.

Tutkimuksessa löydettiin 15 erilaista haastetta ja pohdinnan aihetta esimerkkiorganisaatiossa. Näistä käytetyn menetelmän avulla viisi tunnistettiin kaikkein tärkeimmiksi. Tuloksista oli nähtävissä jonkin verran yhteneväisyyksiä verrattuna alan kirjallisuuden kanssa. Tutkimus kuitenkin esittää ennen kaikkea tilannetta esimerkkiorganisaatiossa, jota voidaan käyttää vertailukohtana arvioitaessa muita vastaavia tilanteita.

## PREFACE

This study was the final act at my information and knowledge management studies at Tampere University of Technology. It has been a long road within the TUT campus during the years but from my point of view it has been not only a growing up as a student but also as a person and an individual. This thesis also marks an end of an era, where it is time to take all those lessons learned with me and head up to new challenges.

First of all I would like to thank the target organization of this theses work for giving me the opportunity with this case, not only to do a meaningful thesis work but also a possibility have an in depth look to the global corporate information management division and be a part of it without much earlier experience. It made me understand how many of the theoretical issues from lecture classroom have impact in the real world too. I also want to thank the university for supporting me with the thesis work, especially professor Samuli Pekkola and university teacher Ilona Ilvonen for giving me guidance when needed throughout this thesis work project.

I also want to thank my relatives and friends for supporting and cheering me up with this project. My biggest thanks goes to my dear family for making it able to finish this thesis work and my studies.

Tampere 15.11.2017

Pekka Lehikoinen

## CONTENTS

1.	INTRODUCTION .....	1
1.1	Research background and motivation.....	1
1.2	Research problem and expected results .....	2
1.3	Research target and scope .....	2
1.4	Research methodologies .....	3
1.5	Research structure and process.....	5
2.	INFORMATION SECURITY .....	7
2.1	Introduction to Information Security .....	7
2.2	CIA .....	9
2.3	Personal data privacy .....	10
2.4	Cloud service security.....	11
3.	RISK MANAGEMENT .....	13
3.1	Risk management process .....	13
3.2	Risk management steps.....	14
3.3	Risk management as a part of information security .....	15
4.	CRM MANAGEMENT .....	18
4.1	Introduction to CRM.....	18
4.2	CRM categorization and features .....	19
4.3	CRM in a cloud .....	19
4.4	CRM environment information security risk management features .....	20
5.	PRESENT STATE FINDINGS FROM INTERVIEWS.....	22
5.1	Target organization.....	22
5.2	Mapping present state via interviews .....	22
5.3	Identified challenges from interviewees .....	26
5.4	Summary of the present state .....	28
6.	INTRODUCING FRAMEWORK USED IN THE STUDY.....	30
6.1	Building up the framework .....	30
6.2	COBIT.....	30
6.3	Octave Allegro .....	31
6.4	Introducing the complete framework.....	32
7.	USE OF FRAMEWORK IN THE TARGET ORGANIZATION.....	37
7.1	How it was used in the organization.....	37
7.2	Interviewee responsible difficulties .....	39
7.3	Handling material and analysis process .....	39
8.	RESULTS OF THE USED FRAMEWORK.....	41
8.1	Results of the analysis.....	41
8.2	Overall findings .....	44
8.2.1	Observations .....	44
8.2.2	Improvements .....	44
8.2.3	Future considerations .....	45

8.3	Most crucial findings .....	46
8.3.1	Lack of resources .....	46
8.3.2	Technical information security by overall architecture .....	46
8.3.3	Stakeholders management .....	47
8.3.4	Shifting into more proactive organization.....	48
8.3.5	Personal data privacy .....	49
9.	ANALYSIS OF THE RESULTS.....	51
9.1	Roots of the issues .....	51
9.2	Cloud service environment .....	51
9.3	Supply chain perspective in CRM.....	52
9.4	Risk management .....	53
9.5	Future considerations .....	53
10.	CONCLUSION.....	55
10.1	Research Conclusions .....	55
10.2	Reliability of the research and its results .....	56
10.3	Future Research.....	57
	REFERENCES .....	59

## APPENDIX A: CRM RELATED INFORMATION SYSTEMS MAPPING

## LIST OF FIGURES

<b>Figure 1.</b>	<i>Research target</i> .....	3
<b>Figure 2.</b>	<i>Research perspective of the study, adopted from Saunders et al. (2009)</i> .....	4
<b>Figure 3.</b>	<i>Structure of the theses</i> .....	5
<b>Figure 4.</b>	<i>House model of Information security governance framework, modified from Da Veiga &amp; Eloff (2007)</i> .....	8
<b>Figure 5.</b>	<i>CIA model, based on Kaufman (2009)</i> .....	9
<b>Figure 6.</b>	<i>Revised KSRM process, modified from Ilvonen et al. (2015)</i> .....	13
<b>Figure 7.</b>	<i>Holistic risk analysis for information security, modified from Spears (2005)</i> .....	16
<b>Figure 8.</b>	<i>Customer information streams, modified from Wilhelm et al. (2013)</i> ....	18
<b>Figure 9.</b>	<i>CRM continuum, modified from Payne &amp; Frow (2005)</i> .....	19
<b>Figure 10.</b>	<i>Public cloud CRM model, modified from Härting et al. (2016)</i> .....	20
<b>Figure 11.</b>	<i>Simplified chart of the CRM environment current state based on interviews</i> .....	25
<b>Figure 12.</b>	<i>Octave Allegro risk management process, modified from Masky et al. (2015)</i> .....	32
<b>Figure 13.</b>	<i>Framework build up from practical viewpoint</i> .....	38
<b>Figure 14.</b>	<i>Different kind of user accounts to the environment</i> .....	48

**LIST OF TABLES**

<b>Table 1.</b>	<i>Interviewed personnel for the study</i> .....	24
<b>Table 2.</b>	<i>Concerns identified from first phase interviews</i> .....	27
<b>Table 3.</b>	<i>Information layers for enterprise security groups, taken from COBIT5</i> .....	33
<b>Table 4.</b>	<i>Risk evaluation parameters</i> .....	34
<b>Table 5.</b>	<i>Relative risk matrix</i> .....	35
<b>Table 6.</b>	<i>Mitigation pool approaches</i> .....	35
<b>Table 7.</b>	<i>Findings scoring, probability and risk pool according to the used framework</i> .....	43

## LIST OF SYMBOLS AND ABBREVIATIONS

CIA	Confidentiality-Integrity-Availability -model
COBIT	Control Objectives for Information and Related Technology
CRM	Customer Relationship Management
ERP	Enterprise Resource Planning
EU	European Union
IoT	Internet of Things
IS	Information Security
IT	Information Technology
KSRM	Knowledge Security Risk Management

# 1. INTRODUCTION

## 1.1 Research background and motivation

Managing and understanding customer data and information has become more and more important domain for many organizations as they are realizing more clearly that different customers have a very different value for the organization (Reinartz et al. 2004). Many organizations invest a lot of resources to collect, store and process customer-based data but they run into a difficulties concerning about the data quality or how to efficiently manage and utilize the gathered data and information (Madnick et al. 2009). Customer relationship management (CRM) can be seen from different perspectives, for example in some organizations, CRM is just a technology solution between different databases or data warehouses while in others it is seen more as a whole method for managing customers (Chen & Popovich 2003).

With customer relationship management there are however a lot of sensitive information about the organization and its customers. With the grown utilization of CRM systems also risks related to the CRM systems information security has grown rapidly (Kim 2010). Because of for example misuse or leaking of the information, there can be serious monetary or imago losses for stakeholders and the organization (Ekelhart et al. 2009). It is often not easy for companies to deal with the risks since organizations have to face a very complex IT environment with issues such as open systems, electronic integration, network interconnections and IT platforms (Kotulic & Clark 2004).

It should be also noted that risk management of information systems is even more important nowadays with various kinds of cyber threats, to minimize the potential risks outcomes and can be even argued that information security risk management is a fundamental concern for companies (Bojanc & Jerman-Blažič 2008). Besides that, Finne (2000) states that business processes are also an important aspect in the area of information security risk management.

There is also a lot of interest in companies to ensure that the individual's rights and information are properly protected in the organization information systems, especially when there are lots of legislation related (Seify 2006). For example EU regulation and directive of personal data protection places heavy sanctions for organizations if a personal data is not being managed properly (EU 2016). To ensure that the information is properly taken into account, the information security management model for personal data protection should include for example access control, operation management of systems, monitoring and auditing (Kwon & Youm 2009).

## 1.2 Research problem and expected results

The target of the research is to study Customer Relationship Management environment's features against the target organization's Information Security. The study is based on two research questions introduced below.

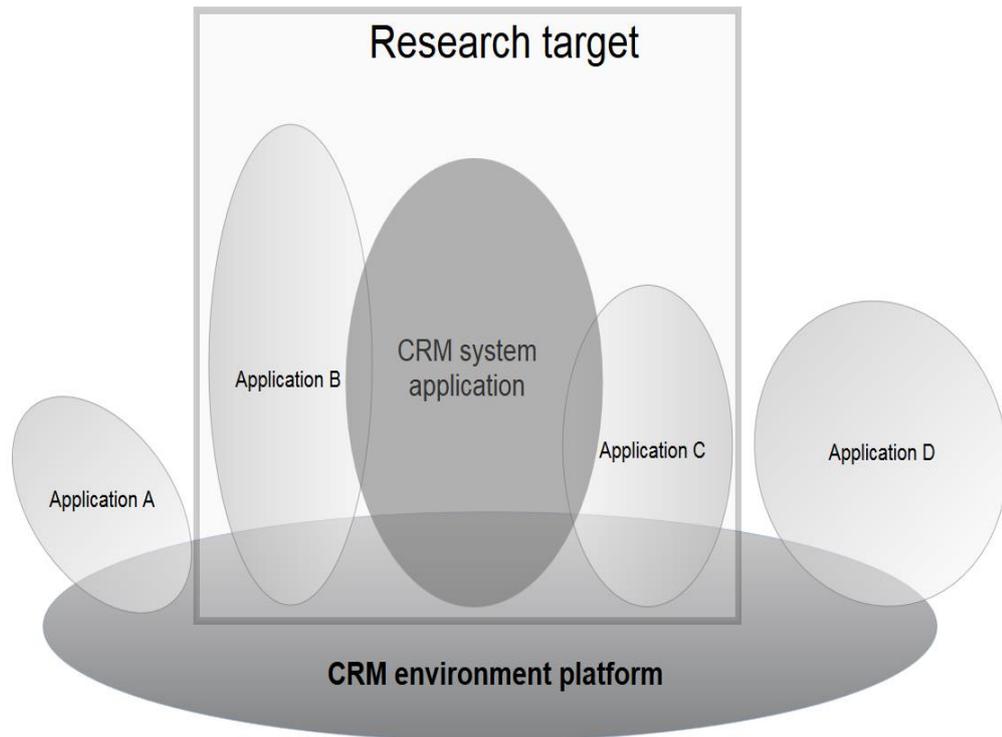
- *“What kind of and how severe risks there can be found in the Customer Relationship Management system environment from organization's Information Security perspective?”*
- *“What kind of responses do the Customer Relationship Management environment risks demand in the case organization?”*

The result of the study is expected to be a mapping of the identified CRM-related information security risks with also proposed responses according to the identified risks. The research is supposed to give a summary of the present state prioritized CRM system information security risks for the target organization. Response propositions for the discovered risks aim to give also proposal on what should be done with the risks, for example are there immediate actions required, further research needed or is there things that need extra consideration. It is also quite possible that the founded risks are already being under observation and new responses are not needed but this scenario belongs to the risk response research question category nevertheless.

## 1.3 Research target and scope

Research scope lies within the organization's CRM system platform environment including related processes and user actions. CRM system platform includes many different applications in addition to the main CRM system. Some of the applications are closely related to the CRM and others share just a same technological platform.

The main focus of the research is based on CRM environment so research will concentrate on the actual CRM system, however other platform applications will be also included if they share CRM methods with the actual CRM application. This leaves out applications that use the same platform environment, but are not related to the CRM system or CRM management. Research scope of the study considering the information system platform is demonstrated in the figure 1 below.



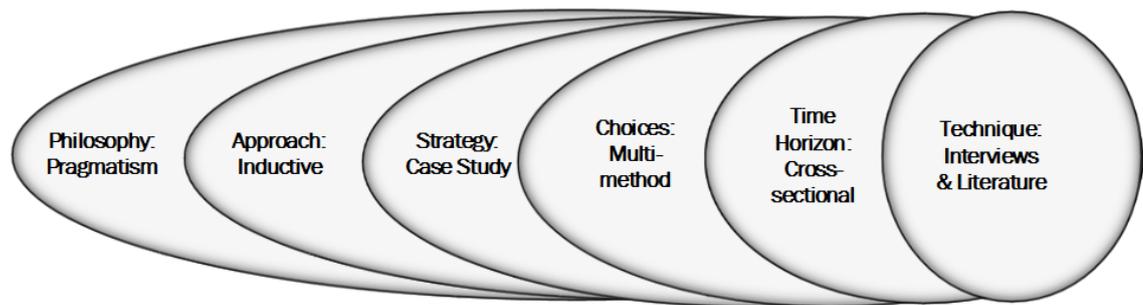
*Figure 1. Research target*

Even if the research target is focused on the CRM system and related applications scope is not limited only to the application functionalities or information content but relevant processes and user actions will also be taken into account. This can mean for example the process how certain information in the CRM system is being classified from information sensitivity point of view.

There is also high level of interest especially to the integration points between the CRM related information systems. This means that even if the whole CRM related information systems function have to be known to understood the relationships between the concerning information systems the integration between the systems is emphasized as the vantage point.

#### **1.4 Research methodologies**

Philosophy of the research is pragmatism. That is because main reason for the study is to find practical answers to the research questions (Saunders et al. 2009, p. 109). This follows Tashakkori & Teddlie (1998) that it is more appropriate for researcher to see philosophies as a continuum rather than opposites and that may even avoid researcher from unavailing discussion about concepts of truth and reality from the research point of view. The complete research methodologies of the study are demonstrated below on figure 2.



**Figure 2.** *Research perspective of the study, adopted from Saunders et al. (2009)*

Approach of the research is inductive. Research structure complies quite well with the Saunders et al. (2009, p. 126) illustration of the approach that first you interview sample of personnel to understand what is going on and the essence of the problem and from these results analyze the findings or build up theories.

The strategy for the research can be defined as a case study because it concentrates doing the research in a particular organization from empirical investigation point of view (Saunders et al. 2009, p. 145). It also goes along with Yin (2003) statement that within case study the boundaries of the phenomenon and context may not be clearly visible.

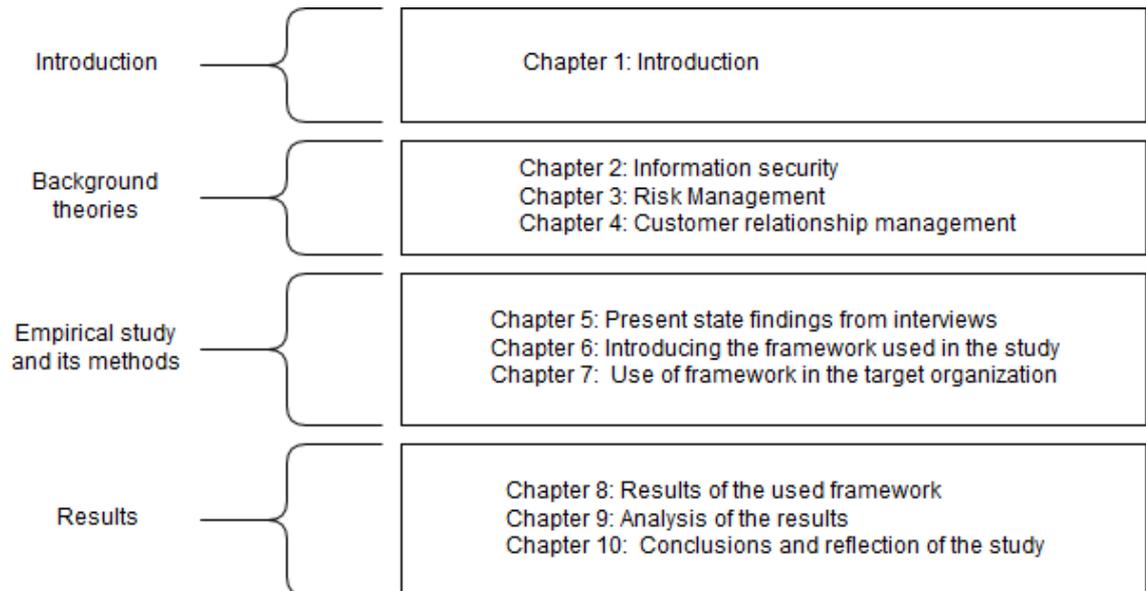
Method choice is chosen to be a multi-method qualitative study. The research is based on multiple methods although emphasis is on interviews, but the analysis is done based on qualitative method, hence multi-method qualitative study.

Time horizon of the study is cross-sectional. The research takes place only on present state of the phenomenon. As the object of the study on in practice under constant change and the research is time consuming event this causes some difficulties. However, aim of the research is to give a sort of a snapshot of the certain moment of the phenomenon so according to Saunders et al. (2009) it is defined as a cross-sectional time horizon.

Technique for the research will consist of the following elements and their subjects. Rudimentary studying of the present state situation in the organization is done by open interviews about the subject to a different organization teams and persons. Theoretical introduction to the study subjects will be based on academic literature. The framework for the analysis is based on both academic literature as well as renowned industry methods. The accurate information for the framework will be achieved with a second round of interviews which are done with semi-structured interviews.

## 1.5 Research structure and process

This thesis can be divided into four parts to help to understand the big picture of the study. The different parts and the chapters they consist of can be seen on figure 3 and they are introduced in details after that.



*Figure 3. Structure of the theses*

First part is introduction where brief introduction to the thesis work subjects will be given. In this part the research target, scope, questions and methodologies will be addressed.

Second part consists chapters 2, 3 and 4. These chapters cover the background theories used in the study from three aspects. These are on chapter 2 information security, on chapter 3 risk management and on chapter 4 customer relationship management. These chapters are based on literature and act as a spine for the further discussion in the study. In this part there is also discussion considering of linking these three aspects together.

Third part consists chapters 5, 6 and 7. In chapter 5 there will be a mapping to the company's present state at the given subject based on empiricism. In practice this is done by open interviews to company's representatives. In chapter 6 framework used in the study is introduced and opened up. In chapter 7 the utilization of the framework also in practice in the target organization will be addressed.

Fourth part consists chapters 8, 9 and 10. Chapter 8 consists results of the framework used in the study for the target organization. The findings will be reported here and each of the most important findings will be highlighted and discussed more thoroughly. In chapter 9 the meaning of the results will be analyzed and discussed. In chapter 10 conclusions and reflection of the study is given.

## 2. INFORMATION SECURITY

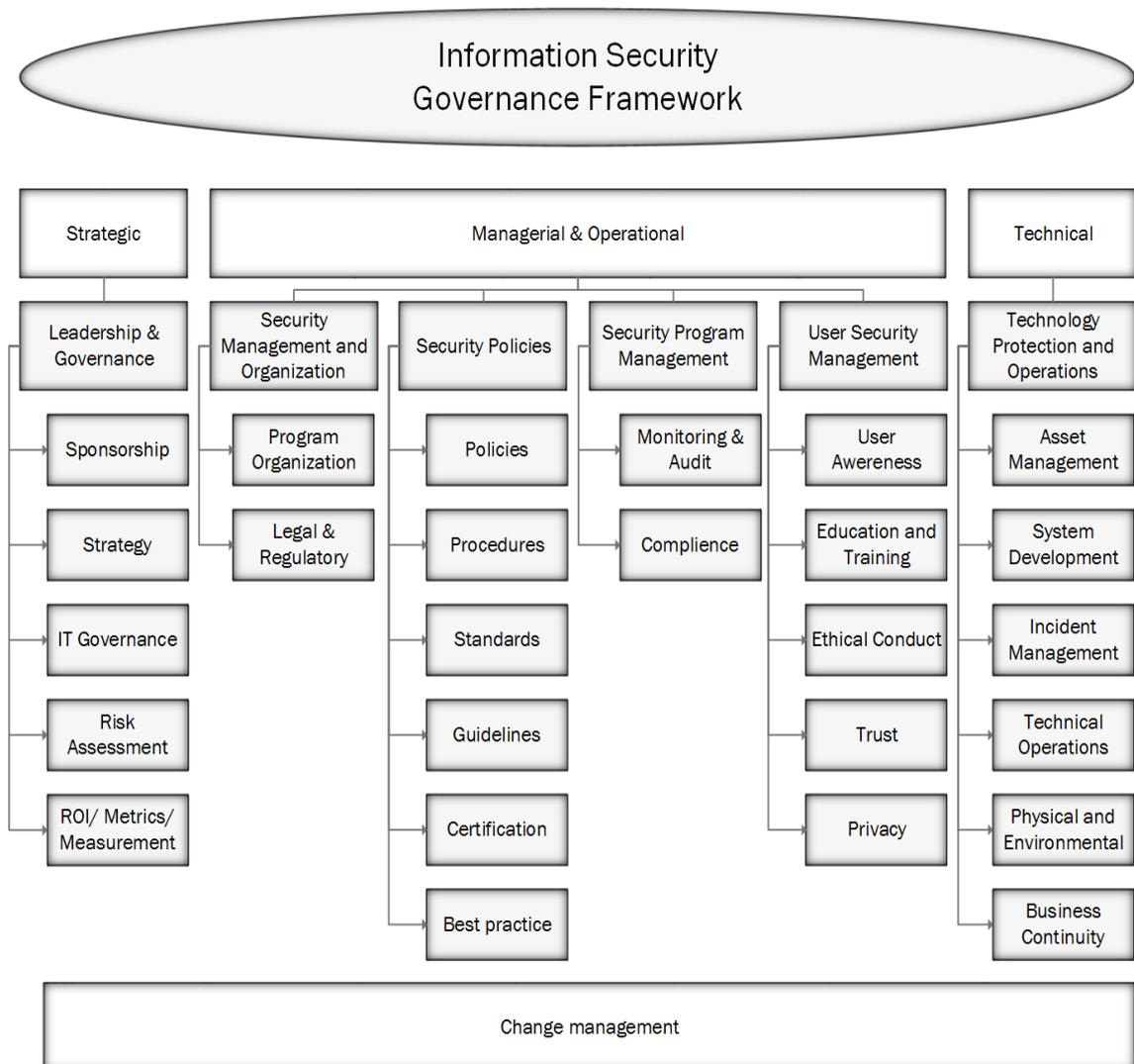
### 2.1 Introduction to Information Security

As many businesses are becoming more and more information related the need for information storing, sharing and utilizing have increased tremendously. This alone has increased the importance of the information security but what emphasizes its meaning is the technological advancements that bring a whole another level to the information security management. Studies have also shown that information security issues have increased during the 2010s even when organizations are investing more money into the information security technologies (Bulgurcu et al. 2010).

Even if there are many kind of technological solution available, information security is still a big issue in practice for many organization which indicates in itself, that information security is not only a technical issue but also a managerial and behavioral (Von Solms & Von Solms 2004; Abhishek et al. 2014). For example, internal staff can often be identified as the most vulnerable source for information security issues, which emphasizes the behavioral and social side of making secure information systems in practice (Hedström et al. 2011). However, personnel in organization can also become a huge resource for making information security more secure if they are able to comply with the security policies and regulations as well as understanding the values that drives for efficient information security management (Bulgurcu et al. 2010; Hedström et al. 2011).

What is also typical for information security in today's business in many industries, is that it is often closely related to other stakeholders too. It is not so easy to create distinct boundaries of the information security to for example on your own organization as in practice for example your partners in business also might share some of your confidential information which makes information security dependent on your partners too (Karlsson et al. 2016).

As it can be interpret from above, information security can be a very complex system with multiple possible components and approaches, especially in large organizations. De Veiga & Eloff (2007) illustrates this wholeness with their house model of the information security governance below in figure 4.



**Figure 4.** House model of Information security governance framework, modified from Da Veiga & Eloff (2007)

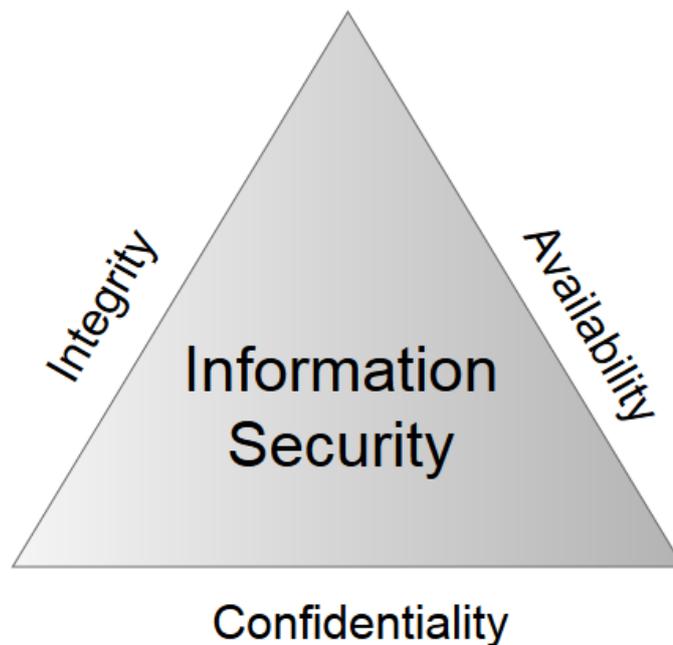
This model shows the many various components of different areas in organizations where information security should be considered or taken into account. This house metaphor is to especially emphasize the idea, that information security is as strong as its weakest link and that is also the reason why information security measurements aren't often that useful (Da Veiga & Eloff 2007). This means that if one of the information security components, the windows in the model, is vulnerable it doesn't matter how strong the other information security components are since the intruder can still already have gotten in. This allegory of the model is especially true when talking about the information security of the cloud computing systems (Kaufman 2009).

This study treats with many of these components described in the house model of information security. Although because as we can see that information security deals with numerous kinds of different perspectives and processes in the organizations there are some components that are given a bit more concentrated view in this study even if there aren't any strict limitation made in this area. Focus will be especially on components like

risk assessment since one of the main targets of the study was to identify found risks and evaluate how severe they were. There is also emphasized interest to for example procedures and processes as well as organizational aspects for understanding the reasons for the study findings rather than concentrating on technical details regarding to the information security.

## 2.2 CIA

More universal perspective to approach information security is via CIA classification. Abbreviation of CIA comes from confidentiality, integrity and availability. Almost all organizations may suffer from unauthorized data observations, incorrect modifications of data and data unavailability and that is the reason why information security must meet the three requirements, which are confidentiality, integrity and availability (Bertino & Sandhu 2005). These three terms form the information security triangle as we can see below on figure 5.



*Figure 5. CIA model, based on Kaufman (2009)*

Within this CIA-triangle method, we can analyze the information security topics with the help of these three terms. Some studies expand this method into a more complex one by adding more elements to it, for example Zhou et al. (2010) add control and audit to it while Xiao & Xiao (2013) make additions of accountability and privacy to it. However the basic three-term CIA method was chosen to be the main viewpoint for information security in this thesis work as, because usually those three can be found in almost any kind of application environments (Bertino & Sandhu 2005).

First aspect in the CIA is confidentiality. Confidentiality in the information security can be in principle seen as keeping the information secret (Zhou et al. 2010). It should be also kept in mind, that software confidentiality is as important as data confidentiality when observing the big picture (Zissis & Lekkas 2012).

Second aspect in CIA is integrity. Integrity in the CIA method is mainly associated with the improper data modifications, which can be caused by for example unauthorized data modification or the or the updated data is not semantically correct (Bertino & Sandhu 2005). The reliability of the data is often very important to the organizations as it was discovered to be the most important section in integrity in a survey for information security professionals (Qingxiong et al. 2008).

Third and final aspect in CIA is availability. Availability can be seen as the ability to reach the information reliably by an authorized actor in a timely fashion (Webb et al. 2014). Availability can be divided into three smaller availabilities, which are data, software and hardware availability, which all should be functioning properly for accessibility and usability on demand (Zissis & Lekkas 2012).

CIA perspective is used in the as a theoretical spine when evaluating cases and issues from information security point of view because of its universal nature. Whereas information security house model can be used to organize and to structurize information security and its different components and areas, CIA perspective is better used to understand the nature findings or to detect the findings from information security point of view.

### **2.3 Personal data privacy**

Personal data and its privacy have had very much interest because of it's highly potential benefits but also because of the threats regarding them (Libaque-Saenz et al. 2016). Personal data privacy regards many of the vital information for organizations that is needed from them to efficiently operate, these can be such as personnel, customer and supplier information, order information and account information (Hilton 2009). Majority of this kind of data is being transferred daily between or within organizations but some of the data can be very sensitive and should be protected, whether because of the special nature of the data for organization or person or by law regulation (Hilton 2009). With the more advanced use of these kind of data brings also more challenges to the organizations since knowledge gathered regarding or from personal data cannot be seen only as a property but also as an individual attribute and part of personality, which may be governed by privacy laws (Dulipovici & Baskerville 2007).

However, privacy as a concept can be sometimes difficult to define precisely (Hilton 2009). It is quite possible that it can be often mixed up with the confidentiality from the CIA-method but there are some differences between them (Bertino & Sandhu 2005).

There have been also identified challenges with the personal data privacy regarding personal data managing. These included figuring personal data as a secrecy, bureaucraties regarding to it and its handling as well as how it is controlled in organizations (Purtova 2009). These sort of privacy concerns and risks related to them have become one on the biggest obstacles for organization to utilize the customer related data they are dealing with their processes (Libaque-Saenz et al. 2016). They have been also identified as one of the reasons for individuals lack of eagerness to participate activities with organizations where personal data are being related (Libaque-Saenz et al. 2016).

Because of the reasons discussed above, it is quite obvious why organizations have today a lot on interests regarding their usage of personal data and its privacy. This is also the reason why it is highlighted and kept in mind in this study even if it not one of the main targets in this study since it is a complex area that would need study of its own to handle it very thoroughly.

## **2.4 Cloud service security**

As cloud computing services are getting a getting more and more used in organizations (Martens & Teuteberg 2011) and they have clearly their own benefits but with cloud computing services there also comes along information security issues (Zhang et al. 2010). As the objects of the study maintains cloud service environment there are few cloud security related topics that should be taken into consideration.

First it should be noted that confidentiality is one of the most important concerns regarding cloud service security, since with it customer is basically outsourcing their data on cloud services which are operated providers that might prove to be untrustworthy (Xiao & Xiao 2013). Cloud service confidentiality can also be emphasized because of the high number of different parties, applications and devices that offer point-of-access to the cloud (Zissis & Lekkas 2012).

While cloud services make use of many concepts, such as SOA (service orientated architecture) or virtualization, it can also inherit the threats related to those concepts (Hashizume et al. 2013). These kind of additional threats pile up with the related topics discussed above making the information security in the cloud services even more highlighted. Clouds can also form large entities and it should be kept in mind that especially with cloud service security, the cloud is as secure as its weakest link (Kaufman 2009). What makes those challenges discussed above even greater is that cloud computing services are often outsourced to third party organizations which often makes the confidentiality, integrity and availability triad harder to properly achieve (Zhang et al. 2010).

Cloud service security is a major aspect in this study from the information security point of view because to the case of organization CRM environment is built primarily on cloud service technologies. Concept of cloud security bring its own characteristics to the table

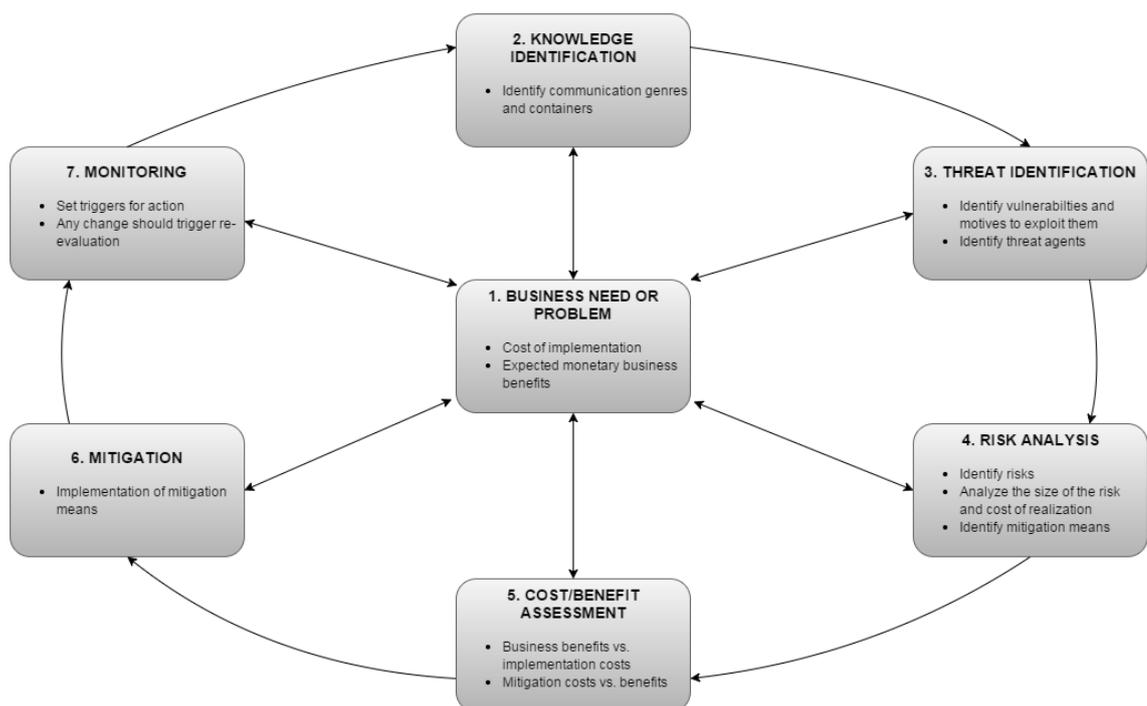
from information security point of view has it has been discussed above. As some of the studied CRM environment features comes directly from the cloud service properties, it is important to recognize and understand matters from cloud service information security point of view too.

## 3. RISK MANAGEMENT

### 3.1 Risk management process

Risk management basically means the process of understanding and efficiently managing the unexpected variabilities that might happen and efficiently managing them with for example implementing mitigation plans (Paquette et al. 2010). This process can have various ways of implementation in different organizations but there are usually at least four recognizable phases (Ilvonen et al. 2015). These four phases are 1) asset and risk identification 2) risk analysis 3) risk-reducing measures and 4) risk monitoring and even if the naming of these phases may differ between the methods their core meanings can be identified and are quite similar (Ilvonen et al. 2015).

In this study risk management process is being approached from a KSRM (knowledge security risk management) process point of view, by Ilvonen et al. (2015). Conceptual model of the revised KSRM process can be seen below on figure 6.



*Figure 6. Revised KSRM process, modified from Ilvonen et al. (2015)*

The four risk management core phases can be identified from the model in question but it is also a bit more detailed model as having seven different steps. The strong linking to business in each step is also noteworthy which supports the subject of the study since according to von Solms & von Solms (2004) not realizing that information security is a business issue and not a technical thing is one ten deadly sins of information security. As

the study takes place on information technology environment the main four steps of the risk management are presented below, particularly from information technology point of view.

### **3.2 Risk management steps**

The first step is identifying risks. Purpose of the risk identification is to proactively discover and determine the internal and external threats for the organizations information technology environment. To efficiently perform this, it is advised firstly to define the IT environment and for example divide into three layers (application, organizational and interorganizational) and analyze threats found from each layer. (Bandyopadhyay et al. 1999)

The importance that the risk identification have to be done controlled so that the findings would be reliable is also noteworthy (Schmidt et al. 2001). For example checklists can be used to help managers or team leaders in this tasks because information systems risk identification often needs people to thoroughly understand the environment which they are dealing with, which is not always the case (Schmidt et al. 2001).

The second step is analyzing risks. Risk analysis methods can be divided into a three categories, which are quantitative approaches, qualitative approaches and combined methods of the quantitative and qualitative approaches (Bandyopadhyay et al. 1999). Regardless of which kind of method is being used, the evaluation of the most important risks that need actions is one of the key aspects of information security risk management (Schmidt et al. 2001).

This whole step can be seen as a three-step process, which consists of what is the risk, how possible it is to happen and how much does it will do damage in one way or another if that risk actually occurs (Gerber & von Solms 2005). Even if this is done controlled and sophisticated, and whether quantitative or qualitative methods are used, it should be remembered that after all it is still more or less just a sophisticated guess (Gerber & von Solms 2005).

Third step is mitigating risks. Risk-reducing methods can be divided into five categories, according to which type of risk are they meant to mitigate (Bandyopadhyay et al. 1999). These five type of risks are natural disaster, data security risks, computer viruses, strategic risks and legal risks and the methods they cover are for example password control, data encryption or employee education.

Even if the possible risks are being mitigated by for example avoiding or transferring it, reducing the possibility or trying to detect it early, there is still always a residual risk, which means that there is always a possibility that it still can occur (Gerber & von Solms

2005). It should be also remembered that adding more mitigation ways often also increases the costs so risk mitigation is usually a balancing between costs and benefits (Ilvonen et al. 2015).

Fourth step is monitoring risks. Risk monitoring is another safeguard where the mitigation methods are being watched and evaluated if they are meeting the expectations and if necessary adjustments will be made so that the organization is prepared appropriately against the risks (Bandyopadhyay et al. 1999). The monitoring should be long term and if the use of the system or technological attributes change it might have to be re-evaluated (Ilvonen et al. 2015).

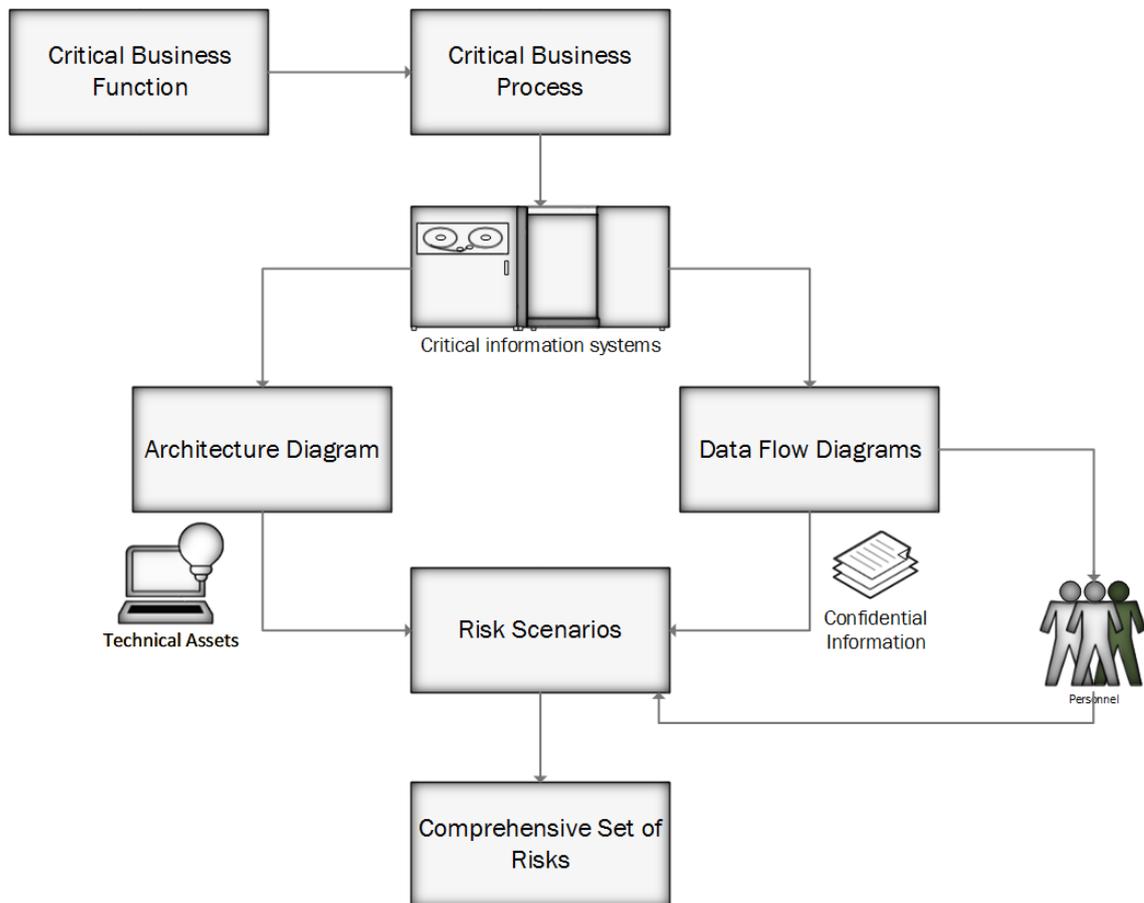
### **3.3 Risk management as a part of information security**

Basically, information security risk management (ISRM) is the process that ensures that the CIA principles are taken into account in the organizations (Webb et al. 2014). These principles should give a good starting point to information security risk management even if Schmidt et al. (2001) state how the most important subjects in the area is under constant change as the technology and processes evolve.

As it can be seen as crucial for organizations to secure their business information, it is also necessary to a plan for the information security risk management (Abhishek et al. 2014). There are several different information security risk management methodologies and approaches used in the industry, for example ISO 27005, OCTAVE, CRAM or ISF to name a few. Organizations often use one method as a baseline for their information security risk management but even if those methods approach information security from a bit different point of view or focus on certain aspects the differences in a big picture are often quite minor (Fenz et al. 2014). Following the risk management main principles discussed on earlier chapter information security risk management methods also usually includes some basic steps that are necessary for the risk management in the information technology environment. There can be usually found some sort of system characterization, threat and vulnerability assessment, risk determination, control identification and control evaluation and implementation (Fenz et al. 2014).

There are of course also some challenges typical to this given area that organizations are facing when implementing their information security risk management strategies on practice. In their study Fenz et al. (2014) researched the problems organizations were facing regarding to the subject and identified major challenges. These challenges included such things as problems with assets management, problems predicting the risks, the overconfidence effect, knowledge sharing, and risk vs. cost trade-offs. It should be also noted, that if the chosen method is not implemented appropriately with considering the actual work practices it is highly possible that the information security policies and practices might be ignored or a not valid workarounds will be created (Hedström et al. 2011).

To efficiently manage the challenges discussed above, there have been introduced a framework for holistic approach of risk analysis for information security (Spears 2005). The basic principles of the framework can be seen below on figure 7.



**Figure 7.** Holistic risk analysis for information security, modified from Spears (2005)

The holistic risk analysis for information security by Spears (2005) goes along with revised knowledge security risk management by Ilvonen et al. (2015) by recognizing business as the starting point for the risk management process. Spears' framework especially emphasizes dualistic nature of information security as dividing the observed process and system into technical architecture and the data flow including the actually personnel. Then together they form the possible risk scenarios from which the comprehensive set of risks can be identified and evaluated. When doing this it should be however noted that culture aspects may have also influence on how the risks are identified and especially evaluated and which ones are emphasized (Schmidt et al. 2001). This holistic risk analysis for information security also takes into account the personnel user awareness, which can be seen necessary for effective information security (Spears & Barki 2010).

When combining knowledge security risk management process by Ilvonen et al. (2015) with the Spears (2005) vantage points it is quite possible to form efficient information security risk evaluation process. That evaluation process would include the traditional

step by step risk management process or also takes account of the architecture and data flow hazards of the information system from information security point of view. This sort of information security risk management model was also the baseline of information security risk management when necessary to compare issues or ideas that arose in the case study and how they fit in with the risk management.

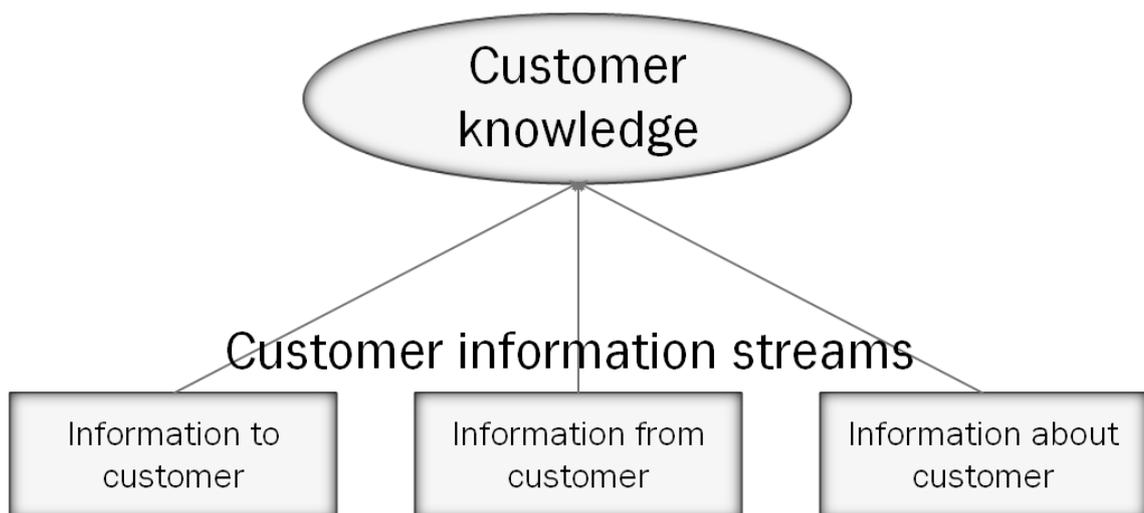
## 4. CRM MANAGEMENT

### 4.1 Introduction to CRM

Customer relationship management has become lately a very important part to organizations, something which has been detected by both researchers and companies. It has become more clear to organizations that different customers have a very different value for the organization. That is also the reason, why it is important to identify customers and groups of customers of how valuable they are and act according to identification. (Reinartz et al. 2004)

It can be defined that to have a successful customer relationship management it is vital to evaluate the actual value of the customer relationship and the commitment of the company (Kim et al. 2006). This can also be seen in practice as many organizations are starting to shift from product or brand based organizations towards customer orientated organizations. It is even claimed that CRM is not only gathering and mixing old practices into a just a new term but actually includes integration of many different activities in organizations and throughout value chain (Boulding et al. 2005).

Customer knowledge can be divided into three information streams (Wilhelm et al. 2013). These are information to customer, information from customer and information about customer. Organization can decide quite effectively what information it gives to customer and what it does not. Customer information streams are illustrated below on figure 8.



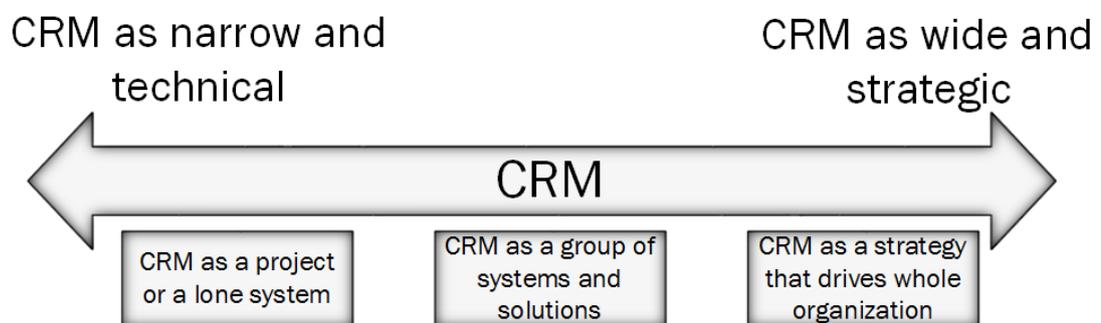
*Figure 8. Customer information streams, modified from Wilhelm et al. (2013)*

Information stream between company and customers can be seen as necessary for the business. There can also be value adding mechanisms founded with the stream, for example customers' needs and complaints can be made of use when adjusting company

strategies. Information about the customers means not only the statistical data like age of person or a location of a company but also for example information about which marketing streams or services customer uses. (Wilhelm et al. 2013)

## 4.2 CRM categorization and features

One way to approach CRM is to see it as a continuum of which can be divided into three phases, although it might be hard to define actual borders for each phase (Payne & Frow 2005). The continuum can be seen in figure 9. On the Left part of the continuum CRM is seen as a project or even as a lone information system. In the middle CRM is a group information systems and solutions for customer information management. On the right part CRM is a strategy that drives the whole organization. (Payne & Frow 2005)



*Figure 9. CRM continuum, modified from Payne & Frow (2005)*

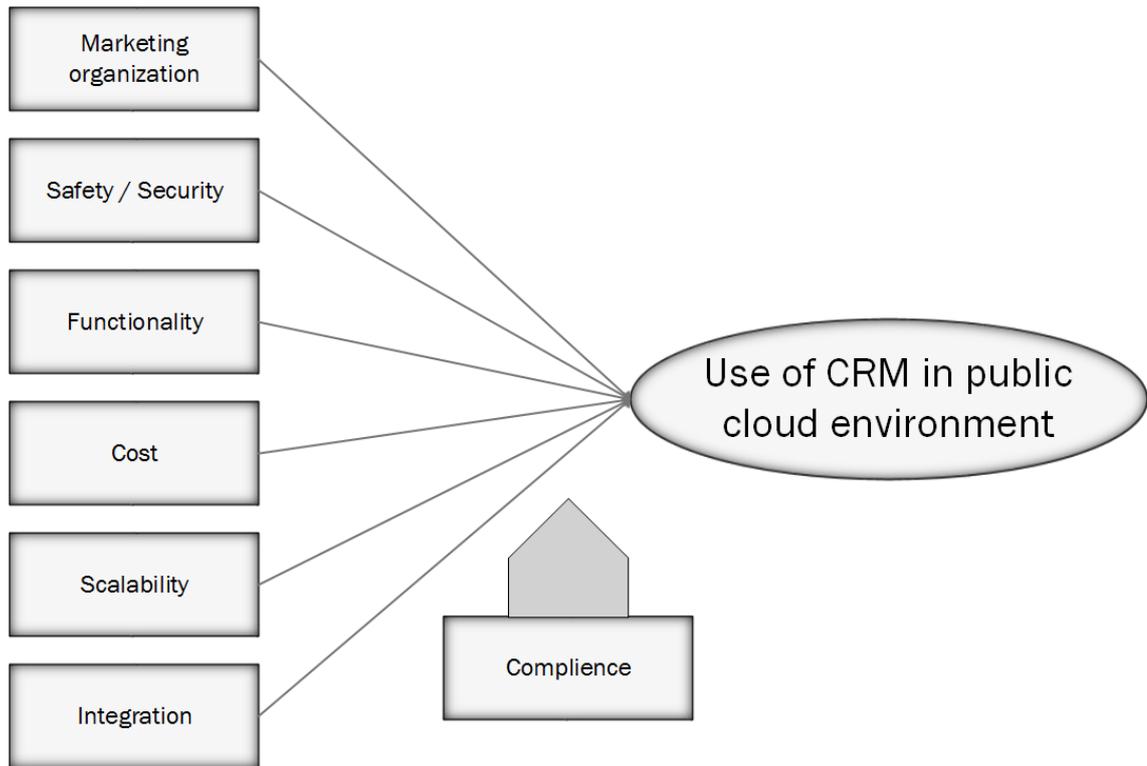
Overall, the definitions of CRM can usually be divided into two categories, strategic and operational. If defined as a strategy CRM combines business to customer management to improve customer profits and loyalty. From operational perspective CRM is seen as a process to manage and maintain data and information of customers in different forms. (Bermejo & Monroy 2010)

In practice CRM is often implemented as a web based information systems in organizations and because of that it can be also seen as a strategic link between the company's marketing strategy and the information technology and department in organizations (Härting et al. 2016). Its purpose can be defined to increase the customer lifetime value for the company by for example segmenting different customers and tailoring their offering based on that (Malthouse et al. 2013).

## 4.3 CRM in a cloud

Recently cloud computing has grown to one of the most important segment in information technology industry because it can extend the capabilities of IT systems without possible for example investing on new infrastructure or training new personnel (Subashini & Kavitha 2011). Härting et al. (2016) found in their study six main reasons for organizations

to use cloud based CRM information systems and one notable moderating effect. Results of that study is displayed below on figure 10.



**Figure 10.** *Public cloud CRM model, modified from Härting et al. (2016)*

The interview experts emphasized marketing organizations, security, functionality, cost, scalability and integration for main reasons for organizations to use CRM in public cloud environment and since all those terms were repeated constantly they can be seen at least as a good starting point for more thorough evaluation (Härting et al. 2016).

#### **4.4 CRM environment information security risk management features**

As it can be seen from the discussion above CRM can be identified in quite numerous ways. In addition, as the CRM environment deals mainly with customer related information which are often very important to the companies financially or strategically or both, it is not surprise that there are interest regarding to CRM environment information security issues. Therefore, it should be first clearly defined in each case separately which objects are under investigation when evaluation the CRM environment information security risk management.

When implementing CRM in a cloud based services as there are done nowadays it is important to scrutinize it thoroughly since its use might be challenging in highly regulated

regions, such as EU for example, because CRM deals with lot of highly sensitive customer related data that is protected by law regulation (Härting et al. 2016). There are for example regulations that certain type of information may not leave from the country and it should be also considered under which jurisdiction the possible investigation will occur (Subashini & Kavitha 2011).

One difficulty is that user may have given permissions to use their data in CRM systems on a certain way or purpose but as companies start to combine their data to use it in their CRM systems for more efficiently those data privacy policies may not align with each other (Malthouse et al. 2013). This causes some questions towards data privacy and security and highlights their role in companies CRM environment (Malthouse et al. 2013). It should be emphasized that security in especially cloud CRM systems is a factor that should not be underestimated and can be seen critical because of the because there are still often found issues regarding topics like data protection and security (Fu & Chang 2015). They bring forth that in their studies they found out that cloud CRM environment was mainly an organizational issues rather that technical issues due to system security (Fu & Chang 2015).

Overall CRM environment in organizations can be seen as an interesting as well as important topic from information security risk management point of view. Due to its nature as sort of a melting pot for many of organization different divisions and processes such as sales, marketing, data management and information technologies for example, CRM environment touches many of these aspects too. This is even more emphasized nowadays since because of the technical development information systems are getting more and more integrated not only conceptually but also technically with each other. Mixing customer data, which can be rather sensitive at times, with sales and purchasing organizations who can be highly integrated to the whole supply chain, gives some of the distinct characteristics to the CRM environment features from information security point of view.

## **5. PRESENT STATE FINDINGS FROM INTER-VIEWS**

### **5.1 Target organization**

The study of the thesis work takes place in a large global industrial company. The company has over 10 000 workers and is represented on different continents. Company's offerings range from items to services on different industrial segments so the variety of different divisions and information systems within the company is quite large. As the company operates and have customers across the globe the information systems also generates a diverse network.

The company has business several divisions, each with their own special features. There are also shared functions for the whole company such as financial or IT divisions. As the study takes place on information systems and their related processes, the study mainly comprises company on corporate group level, if not stated otherwise.

There has been some corporate acquisitions and organizational rearrangements which effects can be seen in company's information systems. Because of the size of the company and the organizational circumstances, there is almost always a constant change going on with the company which should be also noted when evaluating the information systems situation in the company.

### **5.2 Mapping present state via interviews**

In the first phase of the study a present state of the target company's related information systems were identified. This was done via unstructured interviews to the subject related personnel on company's different divisions and functions. The findings of these interviews will be presented more precisely on the next chapter.

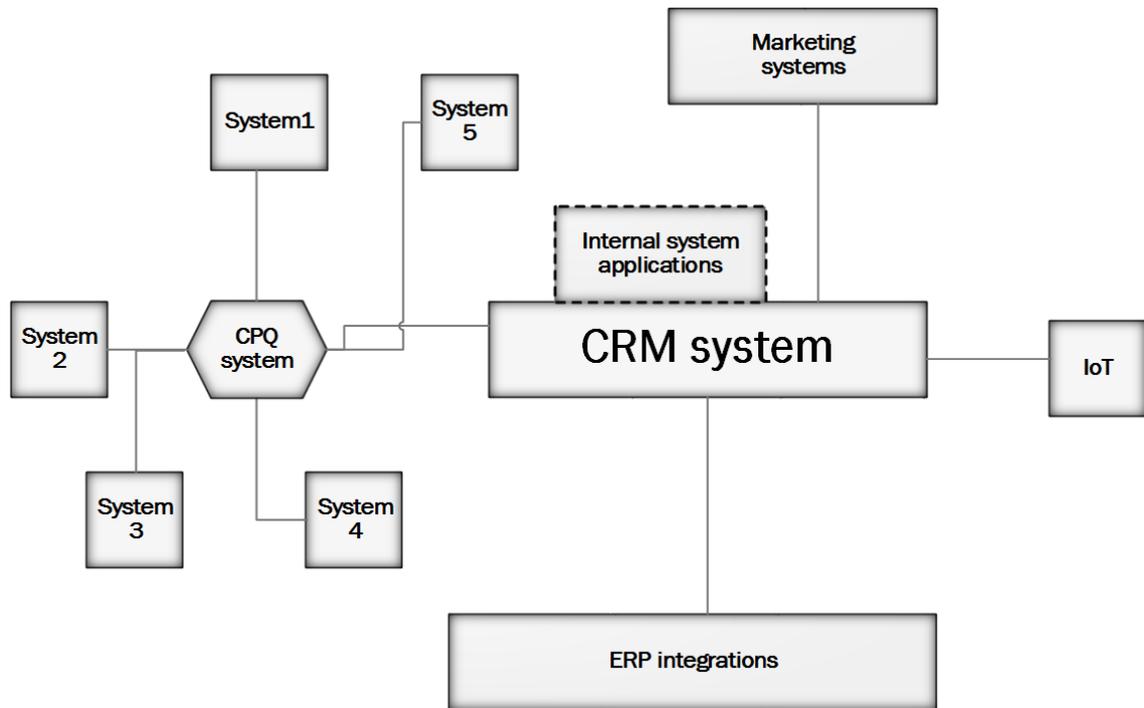
The interviews were done in a face-to-face meetings or via skype due to organization's global nature. Each of the interviews consisted of the interviewer and from one to three interviewee. The interviews were open conversation about the present state from the interviewees point of view and if they had any particular challenges regarding to the subject on their mind. Interviews did not follow any structured pattern to allow the interviewees express themselves freely about the present state. These interviews were done to find out for further examination the challenges or typical characteristics of the current CRM information system environment as well as to sort out the possible actions that needed to be done for the study in the next phases.

There were total of 13 interviews done with 15 personnel. The data collected from the interviews were not anonymous but the as the sources of the findings the interviewees will be addressed with codenames, which still somewhat represent situation in the organization, to protect their identity. The list of the interviewees used in this phase as well as later phases or for complementary interviews can be found below from table one along with the rest of the study interview information.

*Table 1. Interviewed personnel for the study*

<b>Interviewed personnel</b>	<b>Date</b>
<i>Financial Personnel 1</i>	1-6-2016
<i>Financial Personnel 2</i>	1-6-2016
<i>CRM Personnel 1</i>	3-5-2016, 15-9-2016, 13-10-2016
<i>CRM personnel 2</i>	3-5-2016, 15-9-2016, 13-10-2016
<i>CRM personnel 3</i>	13-10-2016
<i>Risk personnel</i>	28-6-2016, 6-9-2016, 23-9-2016, 12-10-2016,
<i>Application Expert 1</i>	20-4-2016, 22-9-2016
<i>Concept Personnel 1</i>	24-5-2016, 22-9-2016, 12-10-2016
<i>Application Expert 2</i>	20-4-2016, 13-9-2016
<i>Application Expert 3</i>	7-7-2016
<i>IT Management Expert 1</i>	15-4-2016, 23-9-2016, 12-10-2016
<i>IT Management Expert 2</i>	15-4-2016, 23-9-2016, 12-10-2016
<i>Sales IT Expert</i>	8-6-2016
<i>Service IT Expert</i>	10-6-2016
<i>IT architecture Expert</i>	22-6-2016
<i>Application Expert 4</i>	1-9-2016
<i>Customer IT Expert</i>	23-6-2016
<i>Concept Personnel 2</i>	22-9-2016
<i>Application Expert 5</i>	21-9-2016
<i>Integration Manager</i>	15-9-2016
<i>Total 20 different persons</i>	Total 24 interviews

Based on the first phase interviews there were also a chart for the current state of CRM environment reconstructed. Purpose of this was to act as an acting point when discovering and analyzing the issues related to the CRM environment in the study's second phase interviews. The simplified chart of the current state CRM environment is described below on figure 11.



**Figure 11.** *Simplified chart of the CRM environment current state based on interviews*

Chart here demonstrates only the different modules or areas of the CRM environment without going into actual different information systems. Integrations drawn on the chart also expresses more of information stream integrations rather than the actual technical solutions.

In practice the integrations from CRM system to the other information systems were quite numerous and the technological solutions varied from each other. However, when approaching from information streams point of view, there can be recognized few different areas and categorizing by them the simplified map above were able to be constructed.

ERP integrations means quite a few different kind of integration between the CRM system and different modules of the organization main ERP system. These information streams consisted mainly of basic sales and customers related data.

Another distinct area was integrations to marketing systems. Different division in the organization had some differing solutions for marketing information systems which also meant the integration were implemented in different ways but together they could still be

categorized as an own area within the integrations due to their marketing related information streams.

Third big different are shown in the illustration is the CPQ (Configure Price Quote) system and its related information systems. This ensemble gathered needed information to CPQ-tool from different information systems, which was interacting then interacting with the CRM system via integration shown in the chart.

One smaller but still different area was the still evolving IoT (Internet of Things) systems integrations to the CRM environment. This area was still very much developing but as it showed whole different kind of information and also risks related to just them it was evaluated to be shown as an integration area of its own.

Finally, last distinct area in the chart is the internal systems applications. This differs quite heavily from the other identified integration areas as they were not independent information systems integrated to the CRM environment but rather different related applications built on the actual CRM information system platform. Whereas technically they were just a different modules in the CRM platform they were still allocated as their own area in the drawing because from information streams point of view, they could be seen as independent information systems with integrations rather than being just a parts of the program.

### **5.3 Identified challenges from interviewees**

From the first phase interviews there were a cluster of challenges or at least issues related to the CRM information system environment identified. The discovered challenges are presented below on table 2. There is also listed the main source from where these concern were brought forth to show how different parts and division in the organization felt about the CRM information system environment, it should be also noted that several of the concern did come more or less directly from different sources.

*Table 2. Concerns identified from first phase interviews*

<b>Finding</b>	<b>Source</b>
<b>Master data change management</b>	<i>Financial personnel 1 &amp; 2</i>
<b>What data should be kept in secret and who evaluates it for example on some kind of scale?</b>	<i>CRM personnel 1&amp;2</i>
<b>Is Personal Data privacy kept in order?</b>	<i>Risk personnel</i>
<b>Relevant information not found or too much information found</b>	<i>Application expert 1</i>
<b>Complex permission settings due to environment features</b>	<i>Financial personnel 1</i>
<b>Data related laws and regulations</b>	<i>Application expert 1, Risk personnel</i>
<b>Users identification</b>	<i>CRM personnel 1&amp;2, IT personnel 1&amp;2</i>
<b>Data Correctness</b>	<i>Application expert 1, Financial personnel 1 &amp; 2</i>
<b>User management process</b>	<i>Concept personnel 1</i>
<b>Complexity of big picture of administration</b>	<i>Application expert 1</i>
<b>SAP integration features</b>	<i>Application expert 2</i>

The concerns here are represented to show some of the challenges different related interest groups within the organization were dealing the study subject. These findings were also used to guide the study into the right direction. It can be seen that found issues were concerning various topics from quite specific properties into a whole processes and their procedures.

There were also various other issues that were discussed in the interviews with the personnel. However with closer evaluation those topics were determined to be out of the scope regarding to this study and its objectives. Even if they were put under closer look in the target organization, those issues weren't addressed further in within this study.

## **5.4 Summary of the present state**

The findings show that there are several challenges or at least some doubt about the CRM environment security features in different parts of the organization. As the findings also are quite divergent between different divisions or functions it might be because of the lack of information or understanding rather than actual information security issues. With that in mind it became clear that the study should not only concentrate on the observed risks or challenges but rather to clarify which of these findings are actual issues to the target organization and which are just due to lack of information within the personnel. This is even if the lack of information is of course also one sort of issue on its own. This can quite understanding that in big corporations like the case organization here where there might not be any personal links to other division even they are connected to each other by business processes some uncertainties rise from just pure lack of better knowledge.

As there seems to be findings regarding to different kind of aspect of information security, for example confidentiality, integrity and the managing process, the research should emphasize especially to the founded aspects. There were also certain information security or CRM aspects that rose up during the interviews but weren't covered with literature research such as the personal data privacy for example. These aspects were taken a closer look and their theoretical background were added to the study.

Overall the studied information system environment received mixed sentiments during the interviews. There were some who were not concerned about the information security aspects at all, or thought they were handled properly were as some interviewees were highly doubtful if certain information security issues were treated properly. There was any notable distinction on that matter whether the interviewee came from for example information technology team or more of a financial team. What is also notable is there were technical aspects as well as information flow aspects defined in the findings. For example, questions regarding to user identification or data correctness seemed to quite major issues since there were at least three different personnel on each cases who brought up this concern.

There were also some findings concerning on issues or confusion on different information systems within the personnel. However even if they were noteworthy observation regarding to the information systems environment in the target organization, these findings were not analyzed further within this study since they were out of the appointed scope of the research. These observations for example were regarded on financial systems, which had

an integration to the actual CRM platform for transferring certain data needed in the financial business processes. However as data were not related in any ways to the actual customer relationship management, other than that the technical implementation shared the same platform as the CRM information system those issues were decided to rule out of the scope which was set in the beginning when defining the targets and limits for this study.

Present state mapping did fulfill its placed expectations as it gave already by itself a good looking to the situation regarding CRM environment issues. It also worked well to appoint what were the integrated other information systems what should be evaluated more closely. Most of the next phase interviewees contact details were also gathered in this phase during the interviews.

## 6. INTRODUCING FRAMEWORK USED IN THE STUDY

### 6.1 Building up the framework

To evaluate the current situation in the target organization a certain practical framework was developed to make sure the evaluation process would be suitable the case organization and the situation in question. The framework was built on three different point of views. First one was the commonly used methods in the industry, in this case the main interest was on COBIT from ISACA which features are discussed more thoroughly on chapter 6.2.

The other point of view was the academic literature on the given subject. Here the main aspects are already being discussed in previous chapters. It is also notable that academic literature was not being utilized very directly when building up the framework but rather as a principles or guidelines for the framework used in the study.

Third point of view was the practical iteration of the framework with the organization personnel. This was in order the sort out what were the relevant aspects to be evaluated and taken care of in the target organization. In practice this was done so that after mapping the present state the first concept of the framework was produced. This first version of the framework was then discussed with selected organization personnel from different parts of the organization to give their statement and discuss about the framework elements.

After these conversations, the final iterated version of the framework was documented. This is also the version of the framework of which was used to accompany the interviews in this study within the case organization. Below the different elements of the framework are being introduced more thoroughly and finally the actual framework is being introduced.

### 6.2 COBIT

First of the two major methodologies that were used for building up the framework used in this study was so called COBIT methodology. Control objectives for information and related technology (COBIT) is developed by the information systems audit and control association (ISACA). COBIT is one of the commonly used frameworks for information technology systems in organizations (Tuttle & Vandervelde 2007). The idea is that COBIT introduces several information technology related control points and security processes to organizations of which they can monitor and adjust to improve their business

achievements and internal control while also reducing their IT related risks and vulnerabilities (Kerr & Murthy 2013).

The idea of COBIT is that it divides IT governance into over different 30 processes that can be then examined independently. Those processes are then divided into more detailed control objectives where there are guidelines how the control objectives should be managed. The bottom line is that if all of the control objectives are managed properly then all the IT governance processes should be in order and the information security in the organization should be properly managed. (Von Solms 2005)

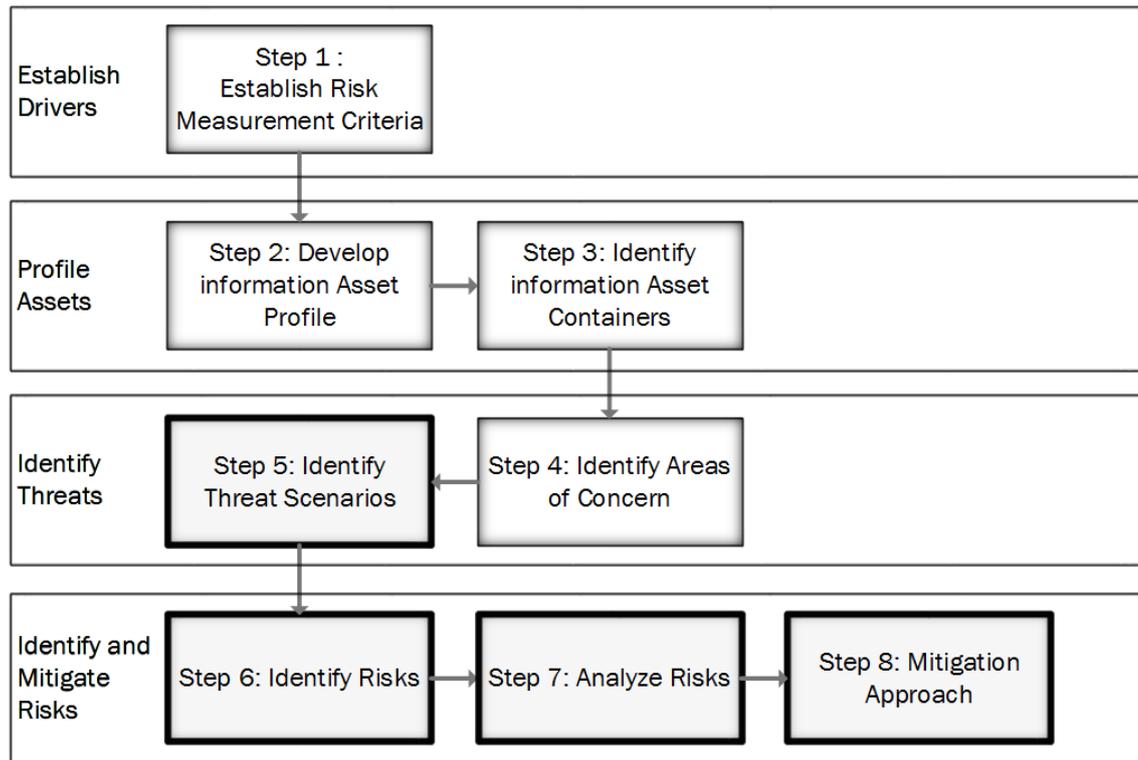
According to Von Solms (2005) one of the greatest benefits of COBIT is that it is not only an information security framework but takes a bit more comprehensive point of view but the downside of this is also that it is not always so accurate in details of how certain things should be done in practice. Tuttle & Vandervelde (2007) also states how COBIT can be, and has often been, used for both internal and external IT-control audits but they would also highlight that it is still not a totally accurate framework from all of the criteria.

### **6.3 Octave Allegro**

The second of the two major methodologies that were being used for building up the framework used in this study was Octave Allegro. Octave Allegro is a risk assessment tool for information systems. Octave (Operationally Critical Threat, Asset and Vulnerability Evaluation) Allegro is one of the available Octave versions. Octave Allegro is a lite version of the more thorough original Octave method and as a such it doesn't need so much expertise or working hours from organization while still concentrating on information assets (Padyab et al. 2014). It is also considered to have quite easy to follow guidelines and its relatively simple method to use (Padyab et al. 2014).

One of the benefits of using Octave allegro in cloud computing environment such as the target environment in this case study is the possibility to move focus into a more information centric risk evaluation and analysis (Masky et al. 2015).

Octave Allegro roughly follows the risk management process which principles were introduced earlier in chapter 3.1. Octave Allegro is divided into four phases and eight steps (Masky et al. 2015). In this study mainly the latter part of the Octave Allegro risk management process was used to help with the risk evaluation, however other steps of the process were also into account when developing the approaches for the study interviews. Octave allegro risk management process is described below in figure 12 and the parts which were mainly used in this study framework are highlighted.



**Figure 12.** *Octave Allegro risk management process, modified from Masky et al. (2015)*

The ease of use of these steps come partly from because Octave Allegro manual have ready a set of sheets and tables for example for the identifying and analyzing steps which can be used as a such or modified for use. For example Pyka and Sobieski (2012) demonstrate how with Octave Allegro you can emphasize organization security priorities in according to the business concerns and weight differently key information assets that suits the target organization.

## 6.4 Introducing the complete framework

As stated earlier the main source of information for the study of the target organization was acquired through various interviews. These interviews were not strictly structured but the elements followed the built up framework introduced here. Main themes for the interviews were gathered from the academic literature introduced before in this study. Different aspects of enterprise information security to cover was based on COBIT5 enterprise security groups described below.

From COBIT5 the information model from the look of the enterprise security groups there are four different layers of the information which should be analyzed when defining the information security.

**Table 3.** *Information layers for enterprise security groups, taken from COBIT5*

<b>Layer</b>	<b>Description</b>
<i>Physical layer</i>	How and where is information physically stored?
<i>Empirical layer</i>	What are the access channels to the information
<i>Semantic layer</i>	What type of information is it? Is the information current or relating to the past or to the future?
<i>Pragmatic layer</i>	What are the retention requirements? Is information historic or operational?

To support the analyze and comparison of the found results during the study a more structured results were also needed. Here specifically selected parts for the study purpose from Octave Allegro risk analysis method was used. Estimation is based on impact analysis from Octave allegro organizations information security needs.

The found issues are evaluated based on varied version of Octave allegro risk evaluation assessment. First of the three steps here is to score the found asset. Scoring is done by five impact categories of which each one is ranked from 1 to 5. There is also an impact value from low to high, which works as a coefficient to the ranking score. From these builds up score for each of the impact area of which are summed in to create a total score for the asset. The risk evaluation assessment is demonstrated below on table 4.

**Table 4.** Risk evaluation parameters

<b>Impact Area</b>	<b>Ranking</b>	<b>Impact Value</b>	<b>Score</b>
<i>Reputation</i>	1-5	Low(1)-Moderate(2)-High(3)	Ranking*Impact value
<i>Financial</i>	1-5	Low(1)-Moderate(2)-High(3)	Ranking*Impact value
<i>Productivity</i>	1-5	Low(1)-Moderate(2)-High(3)	Ranking*Impact value
<i>Safety and Health</i>	1-5	Low(1)-Moderate(2)-High(3)	Ranking*Impact value
<i>Fines/Legal</i>	1-5	Low(1)-Moderate(2)-High(3)	Ranking*Impact value
		<b>Total Score</b>	Sum of Scores

After the asset scoring has been made the assets are divided into different risk pools based on their score and the probability of the risk. These pools and their divisions are also based on the Octave Allegro tool. There are four different pools from 1 to 4 which are first placed on their risk score calculated on the previous step in the framework and after that their probability on a three-step-scale is being taken into account to determine the final pool for the asset. Probability here means that assets which are evaluated with high probability are more likely to happen actually than the assets that are determined to the medium or low category. This relative risk matrix can be seen below on table 5.

**Table 5.** *Relative risk matrix*

<b>Relative Risk Matrix</b>			
	Risk Score		
<b>Probability</b>	30 To 45	16 To 29	0 To 15
<b>High</b>	Pool 1	Pool 2	Pool 2
<b>Medium</b>	Pool 2	Pool 2	Pool 3
<b>Low</b>	Pool 3	Pool 3	Pool 4

Last step is to determinate the mitigation approach for each asset. This part is based on the pools from the relative risk matrix. The options from Octave Allegro Mitigation approaches are mitigate, defer or accept. For each pool there is a mitigation approach suggested on how they should be handled. The mitigation approaches for different pools can be found on table 6.

**Table 6.** *Mitigation pool approaches*

<b>Pool</b>	<b>Mitigation Approach</b>
<b>Pool 1</b>	Mitigate
<b>Pool 2</b>	Mitigate or Defer
<b>Pool 3</b>	Defer or Accept
<b>Pool 4</b>	Accept

The idea between different mitigation approaches is that if an asset evaluated to belong into pool one it should be considered so severe that it have to be mitigated in a one way or the other. The framework itself doesn't tell you how the mitigation should be done but it is left under further analyzing and deciding the appropriate mitigation method. Pool two and pool three suggests there can be done case by case estimation if the asset should be mitigated or deferred as on pool two or as on pool three whether it should be accepted or deferred. These asset risks within pools two and three aren't rated as severe as in pool one but there still should be discussion how to deal with them and what should be the appropriate method for that. Pool four means that assets that are evaluated to belong this pool are not severe from their consequences and they are not very likely to happen, so they can

be accepted as such and not further mitigation plans for resources for them are necessarily needed. Of course it can be advisable to at least monitor them too and the features related to the so if the situation changes they can be re-evaluated.

Together these different aspects form the framework used in the study to evaluate and analyze the CRM environment features against the organization information security. In addition to these different steps described above the earlier discussed theories such are also taking into account when evaluating the meaning of the results and their analyzes.

## 7. USE OF FRAMEWORK IN THE TARGET ORGANIZATION

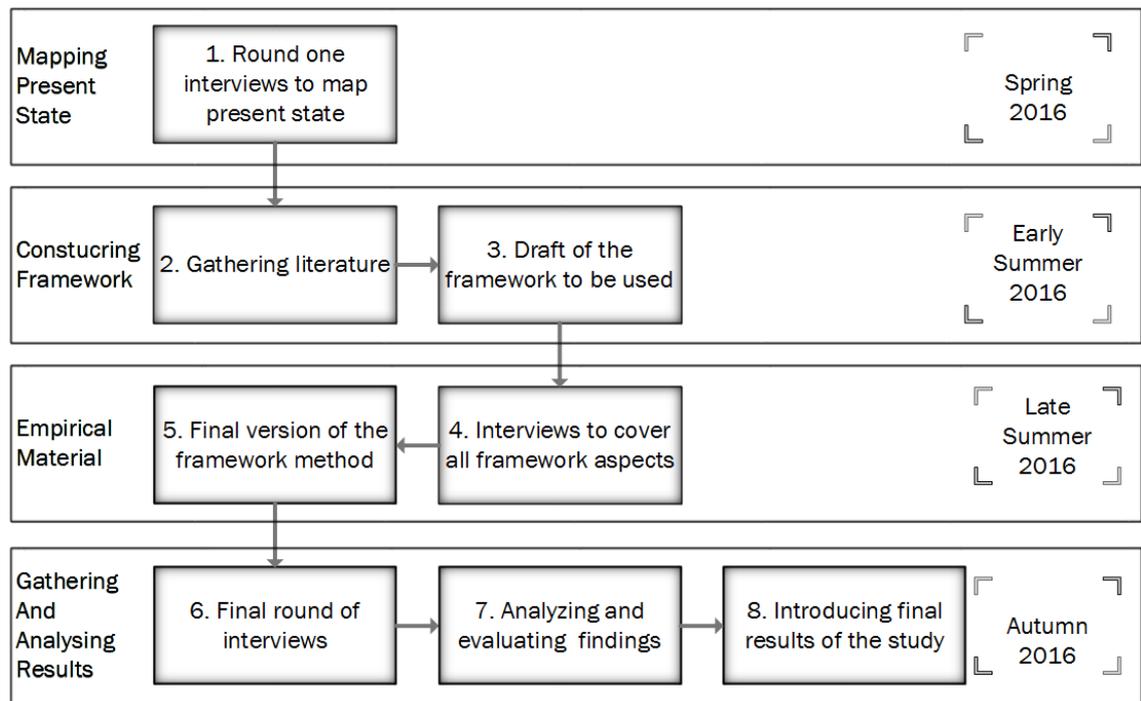
### 7.1 How it was used in the organization

As the purpose of the study was to give a rather holistic picture of the given subject in the target organization and not just focus on technical solutions or issues there were need to collaborate with different divisions and teams of the organization. This was also needed to cover the different aspects of the possible issues introduced in the framework.

As the COBIT5 information layer covers also quite specify information of the data physical attributes there we need to have some technical knowledge from the organization too, even if the emphasize of the study were more on the information point of view.

On the other hand, the Octave Allegro risk evaluation needs estimation especially to the impact of the information on different areas. Here the business and risk knowledge in the organization was very useful and that is also one main reason why representatives from these areas were needed for the study.

Here is described how the study took place and was executed in the target organization from the used framework point of view. On figure the process and schedule is described in a process chart of which shows each of the step of the study process from first phase interviews to the final results of the study.



**Figure 13.** *Framework build up from practical viewpoint*

Teams and personnel to take a part of the study were discovered and selected during the first phase of the study when mapping the current overall state. The selections covered for example risk management, information security, concept managers, various information system representatives as well as integration specialists. However, as the study subject was certain information system environment the selected personnel still represented the related IT personnel from their teams.

When building the framework's first version for the organization literature was also gathered at the same time so that some common topics to the subject from there could be also taken into discussion in the interviews with company representatives. With these discussions it was also possible to develop the framework to the more practical direction with the organization industry experts. There was also some discussion with representatives from other business areas within the organization but after all these parts were left out from the study results as they ended up regarding different functions that were out of the study scope.

After the framework had been consolidated and polished it there were few interviews done again with earlier representatives to test if the changes were proven beneficial and gather material to cover missing aspects of the framework to be used. This was not done in a larger scale and is it was more of a just technical iteration of the framework and interview methods. After these, the final form of how the framework would be used was delivered.

In the final phase there were one last interviews with the key personnel of the subject of the study where aspects and issues that were missing for the final version of framework were completed. After that the analyzing of the results were finalized and the preliminary results were introduced in a couple events where most of the study subject team managers were involved. In these events there were also room for open discussion of the study subjects so that the organization members could also discuss how they felt about the study results in their organization and give their point-of-view on them. This was also important since results from these discussions could be used when reflecting the framework result findings to the common literature of the subject.

## **7.2 Interviewee responsible difficulties**

Gathering up the needed personnel for the interviews had also some difficulties. After mapping the regarding information systems, a responsible person for each information system or feature had to be found from within the organization. For certain areas there were clear appointed personnel or team that was responsible for the given area. However, it also became evident that there was also some lack of knowledge or misunderstanding in some parts about the responsibilities.

Given some time and effort the needed personnel within the organization were found and the interviews were able to be arranged as they were supposed to be. Difficulties relating to quite simple task as finding the responsible persons emphasizes the importance of good documenting of the enterprise architecture. The problem was not that there are not properly pointed personnel but the rest of the organization were at least on some parts unaware, who was in charge of some process or how it was divided between various actors or where to actually get the information.

The above is also important finding in the light of risk management principles discussed in chapter 2. As monitoring of the possible risk was identified as one of the key aspects in the information security risk management environment, named persons should be clearly identified and responsibilities organized so that the monitoring can happen effectively. As part of the interviewing process the difficulties in this area also suggest that risk management monitoring might needed to be also re-evaluated on some cases.

## **7.3 Handling material and analysis process**

The actual material for the study findings were gathered from several interview sessions with organization representatives from different business or responsibility areas. Interviews were done mainly with one or two representatives at time but there were also several sessions where bigger group of representatives where involved. First round on the interviews dealt with mapping the present state of the organization and learning the processes and information systems of the given research area which were already discussed in the chapter 5.

Second round of the interviews were done month or two later and here the actual issues and findings were identified and discussed more thoroughly. Also here interviews were done more commonly with at least two representatives at time to make it possible to have dialogue of the arisen matters immediately with multiple persons and from different viewpoints.

Almost all of the interviews were recorded for further analyze. This was done with the skype meetings or by recording the actual interviews or conversation. All those materials were saved but as they were agreed to use solely on personal purposes the transcriptions aren't available anywhere in this study, however their contents is of course discussed with gathering the material or when analyzing and evaluating the results. There were few interviewees where recording was unable due to technical issues. From these interviewees written notes were archived.

Based on interviews, recordings and notes possible issues and findings were identified and reconstructed to the written formats. These findings were gathered and discussed in further interviews again with the same persons or with also a few arranged meetings where representatives from different areas were gathered together for commenting. This was firstly to ensure that the findings were understood correctly and secondly to overrule that the written findings were only a one time caprice. Because of this all of the findings were discussed at least on two different interviewees during the study, most of them multiple times.

## 8. RESULTS OF THE USED FRAMEWORK

### 8.1 Results of the analysis

After the gathering and evaluation process the results of the study were divided into three categories based on analysis. These three categories were observations, improvements and future considerations according to the nature of the found issue. The findings divided into the three categories are listed below.

- Observation
  - Technical information security
  - Confidentiality classification
  - Permissions management
  - Personal data recognition
  - Shared environment features
  - New applications
  - Stakeholders management
- Improvements
  - Lack of resources
  - Organization collaboration
  - Shifting into more proactive
- Future consideration
  - Information system roles
  - User management
  - Updates
  - Confidentiality highlighting
  - Policies and guidelines

Observations mean clearly distinguished findings that were when gathering and analyzing the material. These are issues that were found to be existing at the moment and their root causes could be fairly well identified. Observations are quite self-explanatory there can be or there have been responsible personnel named to monitor or take care of the problem. Many of the observations were related to the more or less technical limitation or features, whether they were straightforward technical properties or the root cause for them could be tracked to technological properties.

Improvements were findings that were identified during the material analyzing process. Improvements are not necessarily related to just one problem area but there might be several smaller issues on different areas which could be seen to be caused by one of the identified improvements factors such as lack of resources for example. As they are more of an abstract concept rather than for example some technical properties they might be

harder to take care of immediately or by with a straightforward approaches. This category is named to improvements because of the reasons discussed above they should be taken care of constant improving step by step and with collaboration rather than just naming a responsible person and waiting him to take care of the issue.

Last division of the findings were future considerations. In their nature these were more closely related to observations than improvements. What makes them unique in contrast to observations that even if there were issues relating the these findings as they were identified in the material analyzing process they did not too much harms at this stage. However, it was identified that these might cause much more bigger issues in the near future if there wasn't put any effort to investigate them and sorting them out or at least recognizing them and put them monitored. For example user management was still doing quite well at the moment but there were seen issues ahead when the environment keeps on developing if any kind of actions are taken. Because of these reasons this division of findings were named future considerations and kept as a group of their own from observation and improvements.

Below on table 7 the introduced estimations done with the used framework are being introduced. The findings on the table are being identified by the area of evaluation listed above with the calculated scoring according to the framework, estimated probability and the risk pool which is highlighted with different colors according to how severe risk pool they belong to.

**Table 7.** Findings scoring, probability and risk pool according to the used framework

<b>Area of evaluation</b>	<b>Score</b>	<b>Probability</b>	<b>Pool</b>
<b>Technical information security</b>	41	<i>Medium</i>	2
<b>Confidentiality classification</b>	28	<i>High</i>	2
<b>Permissions management</b>	17	<i>High</i>	2
<b>Personal data recognition</b>	39	<i>Medium</i>	2
<b>Shared environment features</b>	14	<i>Medium</i>	3
<b>New applications</b>	10	<i>Low</i>	4
<b>Stakeholders management</b>	33	<i>High</i>	1
<b>Lack of resources</b>	37	<i>High</i>	1
<b>Organization collaboration</b>	13	<i>Medium</i>	3
<b>Shifting into more proactive</b>	35	<i>High</i>	1
<b>Information system roles</b>	14	<i>Medium</i>	3
<b>User management</b>	25	<i>Medium</i>	2
<b>Updates</b>	14	<i>Low</i>	4
<b>Confidentiality highlighting</b>	28	<i>Medium</i>	2
<b>Policies and guidelines</b>	19	<i>High</i>	2

It can be seen that there were findings in every four mitigation pools so there were some highly critical findings identified regarding to their risk status but also some of the findings should not cause too much concerns. These findings are discussed in overall in chapter 8.2 divided into the three categories of observation, improvement and future considerations. Top five most crucial findings are discussed in details in chapter 8.3. These top five most crucial findings were selected by being in the highest part of risk score meaning at least 30 or more while also having probability of medium or high.

## 8.2 Overall findings

### 8.2.1 Observations

From purely technical point of view there weren't much major flaws found in the environment. It is quite possible that this because of there had been few years earlier some successful data breaching to the case organization which is why technical part of the information security had been under highlighted surveillance. There were already done many technical improvements for the information security with for example firewalls and internal internet accesses. So this part might not reflect very the overall situation in the business within other companies.

However, why technical information security was still scored very high in the risk score was because of the technical environment properties which caused some issues for potential information security risks. These were more of the sort that either the business processes and procedures should change to be more according to the platform technical properties or either there should be made some technical tweaks to the platform to better support the business processes used currently. Because they were still caused of by technical properties in the platform they were listed under the technical information security.

During the interviews it was also noted that even if environment information confidentiality policies were up to date the related practices in a big organization were still often lacking behind. For example these policies were written and published in the organization intranet and many of the users were informed about those but the users still weren't adopted them. This was largely due to constant hurry of the other tasks given to user so they didn't have enough time to get to know the confidentiality policies better or that the values behind those were not made clear enough so that there were not enough motivation to adopt them properly.

There were also found variation between practices of the management of the environment profiles and roles between different applications. This was mainly due to insufficient overall architecture management of the accounts permissions sets. There were also different kind of levels to the personal data privacy recognition.

### 8.2.2 Improvements

Improvements were mainly related to the organization culture, structure and resources. However, these were also considered as one of the most important sections to be taken into examination. That is mainly because those identified aspects for improvements where that sort of nature and effect many of the other study findings or even the organizational performance on higher level too so that there should be extra effort on on improving these aspects.

Emphasis of resources and shifting organization culture to more proactive are discussed in details in the most important findings section as they were one of the most important findings in the whole study. However, there were also improvements to be discussed in the collaboration of the environment persons in charge and the project managers or application representatives.

Above highlighted the importance of the discussion and collaboration between different actors in the environment as soon as possible, for example already in the designing phase, to avoid know issues or technical limitations in the environment already before implementation of the processes. This was also seen to be part of the tacit knowledge sharing too because some interviewees felt that lack of understanding the bigger picture functionalities within the organization could be one of the reasons why collaboration weren't find that necessary. It was often left aside under tasks that were more directly linked to the personnel and that's why were felt to be more important.

### **8.2.3 Future considerations**

None of the future consideration made in to the top five most crucial findings. These mainly because as stated before most of the future consideration didn't have high impact on the CRM environment at the moment. Nonetheless there were still some very interesting findings that would be beneficial to take closer look at least on a longer time span.

One of the future consideration identified was the role of the CRM environment versus other organization systems such as ERPs and marketing applications and so on. As the CRM is seemed to becoming even more important to the organization as stated earlier in the study also CRM information system environment is trying to evolve more agile and versatile. There were seen that some functions from traditional ERP or marketing systems were shifted more into the CRM environment. This causes some considerations in the future of how to avoid duplicate work in the organization information systems and to ensure the integrity if the information systems data.

Environment applications and features updates and dealing with those was also took as future consideration. This was noted especially in the light of the organization structure and the responsibilities of keep up with the changes in the environment in a big picture. If platform properties and applications are left to do their updating and developing without a higher perspective to take care of the overall development there is high possibility that sooner or later there are starting to emerge unexpected issues regarding these. Also future updates might cause some issues to already well functioning modules in the platform should there should be enough testing and supervising with the future update to make sure the platform stays stable and reliable.

One other notable findings was the classification highlighting. As the platform is developing and getting bigger and bigger there are also more sensitive information being

loaded to the CRM information systems. This brings lot of questions to how the information classification is implemented in practice in the environment so that all users are aware of how sensitive material there are dealing with and how it should be handled.

## **8.3 Most crucial findings**

### **8.3.1 Lack of resources**

One of the main findings that came up during the study was lack of resources, such as personnel, dedicated working or technological incompleteness. This is certainly not most unique or surprising finding but it cannot be bypassed, since it came across on various interviews and on different kind of situations or problems. What makes it so important is that it have effects on many of the other issues and functions to. Another thing was that with the interviews personnel felt that if nothing would be done to this certain issue it will not repaired by itself with time but rather accumulates and causes even bigger problems.

This was seen distinctly as many of the other found issues were already being identified and were known at least on some parts of the organization but have not being taken care of due to lack resources or lack of dedicated working time as mentioned before. This can also hinder organization quite heavily from acquiring its optimal performance level since even if the staff is experienced and capable enough to identify and even fix the known issues by themselves there just aren't enough time or resources from them to do it.

It was felt very much to be also allocation and prioritizing questioning too. This meaning that different level managers should understand to prioritizing between tasks also on longer time span and from the whole organization point of view. Lack of resources were felt to be also because short term projects that did not have so much impact on bigger scale were prioritized over some bigger and time consuming projects that perhaps were not so urgent but they hindered many other functions. When situation was felt constantly being more or less in this manner the end result the lack of resources to take care of the identified problem where it could be made at least partly with the current personnel if tasks were prioritized differently.

### **8.3.2 Technical information security by overall architecture**

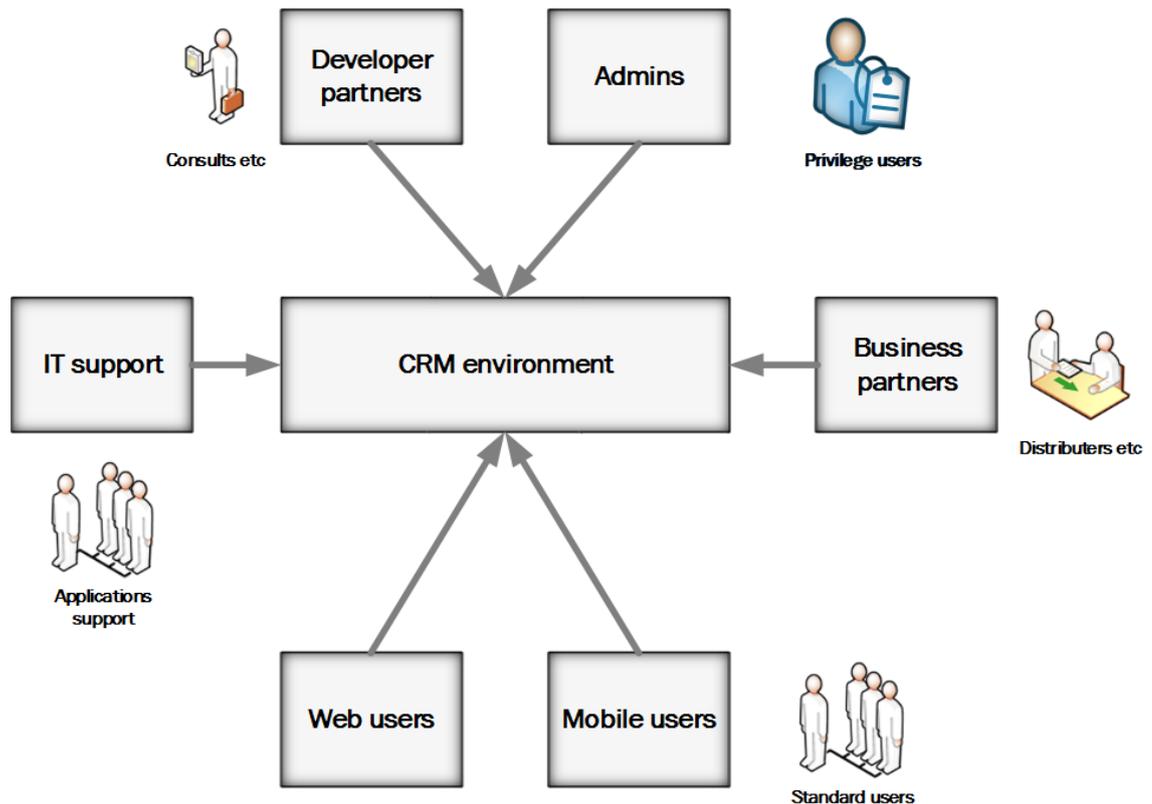
Overall architecture of the CRM environment and its guidance was also found to be an issue. This was found especially when considering the future and evolution of the CRM environment. Even if situation was seemed to be tolerate at the moment where came many issues to be solved in the future that should be dealt with overall architecture in the future. This issue was also related to the top level managers. It was felt that even if different modules and sectors in the CRM environment had their responsible persons set correctly

there were a lack of responsible person to be dedicated to make develop the overall architecture. And also to make sure that different areas and modules were being updated and developed correctly from larger perspective and longer time span.

There were identified risks that all the development and management work was done appropriately there were still lot of what if scenarios found in the future and none felt like having sure answers. This could be also tackled at least partly with stronger overall architecture guidance and monitoring so that there would be also higher responsible person and architecture to where different kind of solution in the development could be compared against to and made sure that the situation would be still within grasps in the future too. These issues where found especially when discussing about the platform and environment expanding and how to make it more controlled and monitored to tackle other minor issues. It was identified that if these sort of question weren't taken properly care of they could many even quite critical information security issues to the CRM environment.

### **8.3.3 Stakeholders management**

Role of third party accounts and personnel in the environment and system was identified as one of the most crucial findings. There were several minor or even major issues related to the management of third party accounts and their personnel that nevertheless were necessary actors to make the environment effective. As the target organization was large global company it naturally had numerous stakeholders with various different kind of user management and access needs. The situation is illustrated below on figure 14 where it can be seen some of the most important different user groups within organization CRM environment information systems.



*Figure 14. Different kind of user accounts to the environment*

For organization it was easier to control its own personnel and their accounts as they could be somewhat estimated and processes were known. However, third party persons outside organization might have to have different kind of roles or needs that weren't needed inside organization or they needed unique kind of settings. Because of these kind of issues, the third part accounts created some issues that were solved in timely fashion but caused customizations and other resolutions that might cause se issues to for example documentation and organizational processes.

There were different solutions and workarounds how these sort of issues had been and could be solved that were used at the moment in the organization. However as these procedures weren't necessary always standardized at least on larger scale it caused some uncertainties that are all user cases dealt properly and where the related documentation could be found or even if there were any. This also highlighted the need of information sharing because there was missing some standardized processes and their documentation as well as the staff being responsible for the whole stakeholder management were felt not to be named clear enough.

### **8.3.4 Shifting into more proactive organization**

Shifting organization on information security related issues from reactive be more proactive was one of the improvements that were identified crucial for the organization from

the information security point of view. As Ilvonen et al. (2015) states for example nowadays knowledge sharing methods make information sharing very easy and fast but also harder to manage, therefore proactive management of knowledge risk should be essential. Even if there were talks in the interviews about changing the culture of the organization into a more proactive regarding risk management there were yet only a few examples of where this was also done actually in practice.

If organization acts mainly as reactive to the information security risks the possible costs from vulnerabilities are harder to decrease and they are easier to control be when proactively reacting to possible threats beforehand. Shifting into more proactive organization doesn't also happen by itself by just trying to change the organizational culture but there also have to be implement processes that ensures that if not constantly then at least periodically the possible hazards are being identified and evaluated. As said before, even if the need for this paradigm shift was already being recognized in the organization, there seemed to be still lot of work to be left to fully put it into practice.

### **8.3.5 Personal data privacy**

Last of the crucial top five findings to be discussed was personal data privacy. Importance of the personal data privacy was highly recognized in the risk management of the organization, mostly due to new EU legislation concerning it (EU 2016). However, when examining more precisely different processes and applications it was obvious that in practice there were still found issues regarding to personal data privacy handling. These potential issues were already being noticed in the management during the interviews it became clear that in the developing teams these aspect might be noted but it was not taken with the seriousness that should be appropriate.

What makes it even more important, and also more challenging, to a global actor such as the case organization is the legislation differences regarding to this subject between different countries. Even if it was taken accordingly into account and test scenarios were made up to date in the CRM environment there were still the need to evaluate it also in other countries where this type of information were needed. There were some scenarios where the differences between the nations regarding these regulations were already found and taken care of but there weren't any systemic study done to this subject within the organization. This can be seen also as a good example of the of how there were still improvement to be done for the organization to shift into more proactive when regarding information security risks as discussed above in the previous chapter.

These issues are also partly related to the cloud service characteristics and the highly integrated CRM feature. This is because of even if many applications or processes doesn't necessary need personal data integration itself the databases and user accounts use same shared environment information and features which might also include sensitive data pri-

vacy. Also the current development is leading to a culture where more precisely information is gathered about customers and other supply chain actors along with the traditional HR-systems it is clear that any issues regarding to personal data privacy in the integrated information system environment should be emphasized.

## **9. ANALYSIS OF THE RESULTS**

### **9.1 Roots of the issues**

Modern CRM information system environment seems to be quite a challenging subject from information security point of view, especially in the case of large organization with complex supply and customer base. As CRM is linked to almost all of the business areas of the organization there are not only numerous integrations to different information systems but also very different kind of data and information regarding for example confidentiality or availability of the data. Still, it seems that even if there were found issues that derives from these features the most important issues were mainly related to organization change management, organizational structure management and user security management.

These findings seem to be quite in line with the basic structures of the House model of Information security governance framework introduced in chapter 3. In the model the basis consisted of change management which seems to have quite big impact also on many of the found issues in the study. Also managerial and operational areas played much bigger role in the model than technical areas which also endorses the findings of the study where technical related issues were rather minor.

What main reason for the found at least minor issues was also the already discussed lack of resources. This is not surprising since in many organizations resources are always limited and divided into different projects and tasks which are under competition with each others about the available resources. Still, like one of the most crucial findings did suggest many of the minor issues were already being noticed and identified at least on some parts of the organization but as there were not enough resources not much had been done with them. So in that mind lack of resources was not only one of the main findings but also root for many of the issues.

### **9.2 Cloud service environment**

Noteworthy issues and considerations relating to user management and permission management can be seen related to the cloud service security. As pretty much all of the information data is centralized to the cloud service the risks of unwanted access to valuable or confidential information is concentrated heavily to the account access management and settings rather than physical equipment management.

It also emphasizes the importance of user and permission management overall architecture and guidelines since users in cloud environment have fewer or even just one account which grants access to the whole information of the cloud service. The access to the cloud have to be restricted by permission and roles rather than having different accounts to different kind of information as is more common in separate information system environments.

This kind of approach to of user and permission management can be seen troublesome to the organization as the study findings suggest. One of the main reasons for that is that because of the reason discussed above cloud service environment emphasizes different kind of access management than the traditional legacy systems especially larger organization tend to have. At least in the case organization the old legacy information systems were more concentrated on certain business processes or user groups meaning two things. First there were not that many different kind of ways of using the information system as the cross-organizational cloud environment information system. Secondly, that also meant that customization and workarounds were often easier to implement to the legacy systems as the side effects were easier to detect and handle because of the more concentrated usage of the information system in certain ways. What came out from the study findings was that organization was struggling how to make sure the different kind of user cases and management was organized when it was a matter of shared cloud environment. In this kind of shared cloud environment platform larger picture of the user access management had to be taken into account because of the larger and more varied user group and use meanings of the platform. This can be seen to be also related to the identified difficulties of the lack of overall architecture and a higher level coordination where organization seemed to still have to learn how to deal with the shared cloud service environment.

### **9.3 Supply chain perspective in CRM**

The next result of the findings analysis was also partly related to the topic discussed above as one of the most important findings were the stakeholder personnel and accounts management in the CRM information system environment. This can be seen related to the paradigm shift of the offerings to customer from just own organization point of view to the whole supply chain offerings. This progress tightens the collaboration consisting also information flows between actors of the supply chain from the contactors and distributors to the customers. This advancement brings new actors also to the CRM environment as the distributors and subcontractors were no longer being dealt with the responsible teams directly but the environment made it possible that they could have straight integration to the organizations CRM environment.

Because of the above it is not sufficient anymore to just define policies and processes regarding to the organization user management but as much of the information needs to be shared across the supply chain the other stakeholder integration to the environment

have to be designed and defined as well. This kind of features in the CRM environment causes a lot of pressure and emphasizes the importance of information confidentiality classification.

It should be also noted that these same issues don't only limit to the supply chain stakeholders but also to many, nowadays even often off-shored stakeholders such as IT support or system development. This is even greater concern since it also come out in the interviews that there was tendency to use even more external resources for different kind of projects and tasks in the organization.

## **9.4 Risk management**

One of the main findings was also the need to shift from reactive information security risk organization to more of a proactive organization. This aims that the possible risks and issues are being evaluated and monitored before they are likely to happen rather than reacting if some of the risks occur.

As there were quite many different kind of challenges or risks identified in the CRM environment either by being already active or had possible consequences in the future, these findings emphasize the role of risk management in this area in the organization. Even if there are risks that cannot be taken care entirely because of for example lack of resources for that or due to nature of the possible hazard it is still very important that risk management identifies and monitors those possible risks. This process as discussed in the theory section covers not only their identification of the risks but also evaluating their impact and by that determining how they should be reacted. If this sort processes are being implanted and are active in the organization it already shifts the organization a big step of being more proactive in the risk management area rather than just being waiting and reacting to happening situations.

## **9.5 Future considerations**

Overall the findings show that as there were not that many urgent critical threats identified and the CRM environment the deployment of the environment was performed quite well and for example were not found much technical vulnerabilities with for example integrations to the other information systems which were one of the main interesting points in the beginning of the study. As most of the identified challenges in the CRM environment were related to the possible future issues with some characteristics it shows that the nature of the cloud CRM environment was not perhaps fully understood at least on certain aspects and what kind of difficulties its nature can bring to the organization.

Identified issues with things like stakeholders management, overall architecture management, information systems roles or future update managements tells that many of the procedures of how the environment was management was still a bit left behind. It shows that

procedures were still clinging a bit of how things were done before and how those managerial choices were not suitable for the cloud service CRM environment and not all the features it brings on were perhaps fully understood.

These findings emphasizes the importance of the proper environment management. As the CRM environment was quite carefully planned not to contain technical vulnerabilities to information security, the inadequate management of the whole environment caused much more severe risks for the environment information security.

## 10. CONCLUSION

### 10.1 Research Conclusions

The research concentrated solely in the target organization and its CRM environment. It was made with several rounds of interviews with the study subject experts from the target organization. Results of the study were 1) a mapping to the present state of the CRM environment and its information system integrations and 2) analysis done from the present state findings of what issues there were found and possible future considerations regarding to the study subject.

Study to the subject present state created CRM related information systems mapping that was demonstrated as an information systems integration graph. The characteristics of each of the integrations was also briefly evaluated to give recommendation if there were issues regarding to that integration that need further analysis. There were three critical information integrations identified that were critical to monitor and four information integrations that were identified with possible information issues. Rest of the integrations were recognized to not contain extra information issues.

From this present state mapping 15 findings were specified and taken into under further analysis. These findings were evaluated by the built framework to estimate of how severe risks did they contain for the target organization. Also a mitigation approach suggestions based on that evaluation were made. Three findings were classified to the first pool to be the most important to be mitigated, seven findings were classified to second pool to mitigate, three findings were classified to the third pool to defer or accept and two findings to the last pool to accept. Based on the evaluation, scoring top five of the findings were also highlighted in the study to give them a more thorough discussion.

Study showed that CRM environment in the target organization had most severe issues on the lack of the needed resources for the environment information security, overall architecture of the complex environment including various integrations also cause issues as well as third party roles management in the environment. Besides these personal data privacy was also highlighted as an area that caused discussion and concern in the environment and lastly the whole shift for the organization to be more proactive rather than reactive regarding the CRM environment information security topics. In addition to these there were five topics that came out from the identified findings which were discussed further to give background for the reasons of these findings. Topics included such areas as roots for the issues, cloud service environment, risk management and so on.

These findings did go fairly well together with the literature findings discussed in the study earlier but there were also some findings that were more characteristic solely to the

target organization. To have more weight on this study findings similar studies should be executed to other organizations to separate better which of the findings are more common to the whole CRM environment from information security point of view and which are more case-specific. However as most of the findings were already highlighted also in the literature it can be assumed that the target organization somewhat represent current state that could be found also in other organizations in the industry.

## **10.2 Reliability of the research and its results**

Even if the aim is to make as objective research as possible, it is notable that the analysis can always be biased, or probably is, especially when research material is principally qualitative rather than quantitative. Also although there have been quite many interviews and the key interviewees have been interviewed multiple times the amount of interviews is still rather small in a large perspective so individual answers and opinions may have higher impact on the results than would be ideal for objective research. This included also such scenarios as for example interviewees might have their own agendas within the organization of which might whether intentionally or unintentionally reflects of their thoughts and answers during the interviews. These sort of possibilities are also good keep in mind especially when judging the importance of the found issues described in the study findings.

It should be kept in mind also that the study was done solely in one organization, even if it was quite big one and major player in its industry. It is still just one point of view to the subject and should be compared to other studies in the given subject from that point of view. There were certain aspects that could be quite credibly identified to be more related just for the target organization used in this case study but there were also various other observations where that could not be recognized that easily. This can cause to some faulty assumptions or generalization to be made in the study because of thinking that they are just representative for the target organization and not to other organization at all or vice versa.

The study was done under just one framework and a study processes related to that. To have some more reliable study results would be to replicate the study with another framework being used. With that it would be possible to compare which of the findings were perhaps too highlighted because the framework that was being used in this study in the target organization. Although there were put quite a lot of effort to make sure that the used process for the study would be quite neutral as there weren't earlier similar study done it quite hard to recognize all the effects that are cause by this chosen study in this particular study.

One aspect in the study was also the constant change of the subject of the research in the organization. The CRM environment in the organization was under constant change and new projects were undergoing all the time. There were already some changes in the

timeframe of the study, as well as some major changes were known to happen in the near future. So even if the timeframe of the study and the interviews were quite short, about few months, and the aim was to make a present state mapping there can also be some level on variation in the results and interviews because of the study timeline.

As the study was also a first rather complex research project for the researcher there is also possibility that because of the insufficient research methodologies some results might be interpreted incorrectly. Also because of this there is also possible that for example interview methods may have not been chosen best for the certain circumstances of which might lead to defective gathering of the data for the research.

### **10.3 Future Research**

From organization point of view, this study was mainly to just map the present state and give some sort of analysis on the status quo of the environment. There would be lot of room for future research for a framework to concentrate on how the situation should be carried on and for example to build a specific road map for the future of the environment, as there is still much development to do.

It might be also beneficial to research more of the personal data privacy and its affection in the CRM environment as it has been quite often touched on briefly in this study. Other studies and news also show that there is increasing interest to this particular subject especially because of its related legislation.

As there were quite a lot of speculation regarding to the different sort of environment management questions, it would be also interesting to do a study about the target organization management structures and cultures. From this kind of study it could be then better analyzed which of the findings are related especially to the CRM environment and are caused by some of its specific features and which are just because of the target organization's organization culture.

To have more knowledge of the actual situation of the study subject in the industry as a whole more similar research to other organizations as well would be required. There can be some assumptions made from this study especially when reflected to the literature in the study subject. With other studies there still would be better chance to compare the results and see if there are any drastic findings between the organizations and to analyze further which might cause them.

Based on the literature research for this study there might be room for more comprehensive study on the actual CRM features discussion from information security point of view. There were some papers regarding it but they gave often quite narrow view or the topic was handled very briefly so more structured and comprehensive approach on CRM information security would be quite beneficial. This is especially since as stated earlier in this

study CRM will probably have even bigger impact in the future and at least there will be more confidential information available in the CRM information systems than there are nowadays usually.

## REFERENCES

- Abhishek, N.S., M.P. Gupta & Ojha, A. (2014). Identifying factors of “organizational information security management”, *Journal of Ent Info Management*, Vol. 27(5), pp. 644-667.
- Bandyopadhyay, K., Mykytyn, P.P. & Mykytyn, K. (1999). A framework for integrated risk management in information technology, *Management Decision*, Vol. 37(5), pp. 437-445.
- Bermejo, G. & Monroy, C.R. (2010). How to measure customer value and its relationship with shareholder value in a business-to-business market, *Intangible Capital*, Vol. 6(2), pp. 142-161.
- Bertino, E. & Sandhu, R. (2005). Database security-concepts, approaches, and challenges, *IEEE Transactions on Dependable and Secure Computing*, Vol. 2(1), pp. 2-18.
- Bojanc, R. & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management, *International Journal of Information Management*, Vol. 28(5), pp. 413-422.
- Boulding, W., Staelin, R., Ehret, M. & Johnston, W.J. (2005). A customer relationship management roadmap: What is known, potential pitfalls, and where to go, *Journal of Marketing*, Vol. 69(4), pp. 155-166.
- Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly: Management Information Systems*, Vol. 34(SPEC. ISSUE 3), pp. 523-548.
- Chen, I.J. & Popovich, K. (2003). Understanding customer relationship management (CRM): People, process and technology, *Business Process Management Journal*, Vol. 9(5), pp. 672-688.
- Da Veiga, A. & Eloff, J.H.P. (2007). An information security governance framework, *Information Systems Management*, Vol. 24(4), pp. 361-372.
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016). L 119. Available: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC>.

- Dulipovici, A. & Baskerville, R. (2007). Conflicts between privacy and property: The discourse in personal and organizational knowledge, *The Journal of Strategic Information Systems*, Vol. 16(2), pp. 187-213.
- Ekelhart, A., Fenz, S. & Neubauer, T. (2009). AURUM: A Framework for Information Security Risk Management, *System Sciences*, 2009. HICSS '09. 42nd Hawaii International Conference on, pp. 1-10.
- Fenz, S., Heurix, J., Neubauer, T. & Pechstein, F. (2014). Current challenges in information security risk management, *Info Mngmnt & Comp Security*, Vol. 22(5), pp. 410-430.
- Finne, T. (2000). Information Systems Risk Management: Key Concepts and Business Processes, *Computers & Security*, Vol. 19(3), pp. 234-242.
- Fu, H.-. & Chang, T.-. (2015). An analysis of the factors affecting the adoption of cloud consumer relationship management in the machinery industry in Taiwan, *Information Development*, Vol. 32(5), pp. 1741-1756.
- Gerber, M. & von Solms, R. (2005). Management of risk in the information age, *Computers & Security*, Vol. 24(1), pp. 16-30.
- Hashizume, K., Rosado, D.G., Fernández-Medina, E. & Fernandez, E.B. (2013). An analysis of security issues for cloud computing, *Journal of Internet Services and Applications*, Vol. 4(1), pp. 1-13.
- Hedström, K., Kolkowska, E., Karlsson, F. & Allen, J.P. (2011). Value conflicts for information security management, *The Journal of Strategic Information Systems*, Vol. 20(4), pp. 373-384.
- Hilton, J. (2009). Improving the secure management of personal data: Privacy on-line IS important, but it's not easy, *Information Security Technical Report*, Vol. 14(3), pp. 124-130.
- Härtling, R.-., Möhring, M., Schmidt, R., Reichstein, C. & Keller, B. (2016). What drives users to use CRM in a public cloud environment? - Insights from European experts, *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 3999-4008.
- Ilvonen, I., Jussila, J., Kärkkäinen, H. & Päivärinta, T. (2015). Knowledge Security Risk Management in Contemporary Companies -- Toward a Proactive Approach, *System Sciences (HICSS)*, 2015 48th Hawaii International Conference on, pp. 3941-3950.
- Karlsson, F., Kolkowska, E. & Prenekert, F. (2016). Inter-organisational information security: a systematic literature review, *Info and Computer Security*, Vol. 24(5), pp. 418-451.
- Kaufman, L.M. (2009). Data security in the world of cloud computing, *IEEE Security and Privacy*, Vol. 7(4), pp. 61-64.

- Kerr, D.S. & Murthy, U.S. (2013). The importance of the CobiT framework IT processes for effective internal control over financial reporting in organizations: An international survey, *Information and Management*, Vol. 50(7), pp. 590-597.
- Kim, S., Jung, T., Suh, E. & Hwang, H. (2006). Customer segmentation and strategy development based on customer lifetime value: A case study, *Expert Systems with Applications*, Vol. 31(1), pp. 101-107.
- Kim, S. (2010). Assesment on security risks of customer relationship management systems, *International Journal of Software Engineering and Knowledge Engineering*, Vol. 20(01), pp. 103-109.
- Kotulic, A.G. & Clark, J.G. (2004). Why there aren't more information security research studies, *Information & Management*, Vol. 41(5), pp. 597-607.
- Kwon, Y. & Youm, H. (2009). Security Management Model for Protecting Personal Information for the Customer Contact Center, *Journal of the Korea Institute of Information Security and Cryptology*, Vol. 19(2), pp. 117-125.
- Libaque-Saenz, C.F., Chang, Y., Kim, J., Park, M.-. & Rho, J.J. (2016). The role of perceived information practices on consumers' intention to authorise secondary use of personal data, *Behaviour and Information Technology*, Vol. 35(5), pp. 339-356.
- Madnick, S., E., Wang, R., Y., Lee, Y., W. & Zhu, H. (2009). Overview and Framework for Data and Information Quality Research, *Journal of Data and Information Quality*, Vol. 1(1), .
- Malthouse, E.C., Haenlein, M., Skiera, B., Wege, E. & Zhang, M. (2013). Managing Customer Relationships in the Social Media Era: Introducing the Social CRM House, *Journal of Interactive Marketing*, Vol. 27(4), pp. 270-280.
- Martens, B. & Teuteberg, F. (2011). Risk and compliance management for cloud computing services: Designing a reference model, *17th Americas Conference on Information Systems 2011, AMCIS 2011*, Vol. 3pp. 2041-2050.
- Masky, M., Young, S.S. & Choe, T.-. (2015). A novel risk identification framework for cloud computing security, *2015 IEEE 2nd International Conference on Information Science and Security, ICISS 2015*, .
- Padyab, A.M., Päivärinta, T. & Harnesk, D. (2014). Genre-based assessment of information and knowledge security risks, *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 3442-3451.
- Paquette, S., Jaeger, P.T. & Wilson, S.C. (2010). Identifying the security risks associated with governmental use of cloud computing, *Government Information Quarterly*, Vol. 27(3), pp. 245-253.
- Payne, A. & Frow, P. (2005). A strategic framework for customer relationship management, *Journal of Marketing*, Vol. 69(4), pp. 167-176.

- Purtova, N. (2009). Property rights in personal data: Learning from the American discourse, *Computer Law & Security Review*, Vol. 25(6), pp. 507-521.
- Pyka, M. & Sobieski, S. (2012). Implementation of the OCTAVE methodology in security risk management process for business resources, *Advances in Intelligent and Soft Computing*, Vol. 118pp. 235-252.
- Qingxiong, M., Johnston, A.C. & Pearson, J.M. (2008). Information security management objectives and practices: A parsimonious framework, *Information Management and Computer Security*, Vol. 16(3), pp. 251-270.
- Reinartz, W., Krafft, M. & Hoyer, W.D. (2004). The customer relationship management process: Its measurement and impact on performance, *Journal of Marketing Research*, Vol. 41(3), pp. 293-305.
- Saunders, M., Lewis, P. & Thornhill, A. (2009). *Research Methods for Business Students*, 5th ed., Pearson Education Limited, England, 614 p.
- Schmidt, R., Lyytinen, K., Keil, M. & Cule, P. (2001). Identifying software project risks: An international Delphi study, *Journal of Management Information Systems*, Vol. 17(4), pp. 5-36.
- Seify, M. (2006). New Method for Risk Management in CRM Security Management, *Third International Conference on Information Technology: New Generations (IT-NG'06)*, pp. 440-445.
- Spears, J.L. (2005). A holistic risk analysis method for identifying information security risks, *IFIP Advances in Information and Communication Technology*, Vol. 193pp. 185-202.
- Spears, J.L. & Barki, H. (2010). User participation in information systems security risk management, *MIS Quarterly: Management Information Systems*, Vol. 34(SPEC. ISSUE 3), pp. 503-522.
- Subashini, S. & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing, *Journal of Network and Computer Applications*, Vol. 34(1), pp. 1-11.
- Tashakkori, A. & Teddlie, C. (1998). *Mixed Methodology: Combining Qualitative and Quantitative Approaches*, Sage, Thousand Oaks, CA, .
- Tuttle, B. & Vandervelde, S.D. (2007). An empirical examination of CobiT as an internal control framework for information technology, *International Journal of Accounting Information Systems*, Vol. 8(4), pp. 240-263.
- Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers and Security*, Vol. 24(2), pp. 99-104.
- Von Solms, B. & Von Solms, R. (2004). The 10 deadly sins of information security management, *Computers and Security*, Vol. 23(5), pp. 371-376.

Webb, J., Ahmad, A., Maynard, S.B. & Shanks, G. (2014). A situation awareness model for information security risk management, *Computers and Security*, Vol. 44pp. 1-15.

Wilhelm, S., Gueldenberg, S. & Güttel, W. (2013). Do you know your valuable customers? *Journal of Knowledge Management*, Vol. 17(5), pp. 661-676.

Xiao, Z. & Xiao, Y. (2013). Security and privacy in cloud computing, *IEEE Communications Surveys and Tutorials*, Vol. 15(2), pp. 843-859.

Yin, R.K. (2003). *Case Study Research: Design and Method*, 3rd ed., Sage, London, .

Zhang, X., Wuwong, N., Li, H. & Zhang, X. (2010). Information security risk management framework for the cloud computing environments, *Proceedings - 10th IEEE International Conference on Computer and Information Technology, CIT-2010, 7th IEEE International Conference on Embedded Software and Systems, ICESS-2010, ScalCom-2010*, pp. 1328-1334.

Zhou, M., Zhang, R., Xie, W., Qian, W. & Zhou, A. (2010). Security and privacy in cloud computing: A survey, *Proceedings - 6th International Conference on Semantics, Knowledge and Grid, SKG 2010*, pp. 105-112.

Zissis, D. & Lekkas, D. (2012). Addressing cloud computing security issues, *Future Generation Computer Systems*, Vol. 28(3), pp. 583-592.

## **APPENDIX A: CRM RELATED INFORMATION SYSTEMS MAP- PING**

*Confidential*