TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

LASSE LAUKKA

INFORMATION SECURITY MANAGEMENT SYSTEM IMPLEMENTATION FOR A CERT

Master of Science thesis

Examiner: Prof. Jarmo Harju
Examiner and topic approved by the
Faculty Council of the Faculty of
Computing and Electrical Engineering
on 8th April 2015

ABSTRACT

LASSE LAUKKA: Information Security Management System Implementation for a CERT
Tampere University of Technology
Master of Science thesis, 44 pages
May 2015
Master's Degree Programme in Information Technology
Major: Communication Systems and Networks
Examiner: Prof. Jarmo Harju
Keywords: CERT, ISMS, ISO 27001, SIM3, Security, Management, Risk, Assessment

This thesis is about implementing an ISMS (Information Security Management System) for a CERT (Computer Emergency Response Team). In this thesis the ISMS is based on the ISO 27000 standard family which is an internationally recognized standard developed by the International Organization for Standardization.

This thesis will provide a clear guideline on how to implement the ISO 27001 requirements for ISMS in an effective way for a CERT. A CERT is a team that is responsible for being the single point of contact when something goes wrong. A CERT usually handles vulnerability coordination, incident response and other information security related areas. It is very important that the level of information security inside the CERT is at a decent level.

The ISO 27001 is a general level standard meant for every organization there is, so it has to be tailored for the use of the target organization. The implementation of the ISMS requires a lot of research and effort if one wants to implement that for a CERT. This thesis provides one way to have the ISMS successfully implemented. However the actual certification is not in the scope of this thesis as it is not often required for a CERT.

TIIVISTELMÄ

LASSE LAUKKA: Tietoturvanhallintajärjestelmän käyttöönotto CERT-organisaatiossa
Tampereen teknillinen yliopisto
Diplomityö, 44 sivua
Toukokuu 2015
Tietotekniikan koulutusohjelma
Pääaine: Communication Systems and Networks
Tarkastajat: Prof. Jarmo Harju
Avainsanat: CERT, ISMS, ISO 27001, SIM3, Tietoturva, Riskienhallinta

Tämä diplomityö käsittelee ISMS:n (Information Security Management System) käyttöönottoa CERTissä (Computer Emergency Response Team). ISMS on tietoturvanhallintajärjestelmä, jonka tarkoituksena on parantaa kohdeorganisaation tietoturvaa asettamalla vaatimuksia tietoturvan eri osa-alueille, sekä parantamalla prosesseja, toimintatapoja ja dokumentaatiota.

CERT on organisaatio, joka on vastuussa organisaation tai sen osan tietoturvaloukkausten ja -tapaturmien selvittämisestä. Lisäksi CERT suorittaa yleensä sen asiakasympäristöön liittyvää haavoittuvuuskoordinaatiota, haavoittuvuusseurantaa, sekä muita tietoturvatoimenpiteitä.

Tämän diplomityön ISMS perustuu ISO 27000-standardiperheeseen. Koko standardiperhe on riskiperustainen, ja pääasiassa koko prosessi pohjautuu riskien tunnistamiseen ja hallintaan. ISO 27001 määrittelee ISMS:n vaatimukset, ISO 27002 sisältää käytännön ohjeita ISMS:n käyttöönottoon ja ISO 27005 tarjoaa ohjenuoria tietoturvariskienhallintaan.

Koska ISO 27000 standardiperhe on yleisellä tasolla kirjoitettu standardi, joudutaan käyttöönottoprosessi suunnittelemaan aina kohdeorganisaation ehdoilla. Tämä diplomityö tarjoaa yhden tavan, jolla ISMS saadaan onnistuneesti käyttöönotettua CERTissä.

PREFACE

A long journey has come to its end. In overall these have been the most consuming six months that I have ever had. Now I am glad to say I got everything done on time. I must say that it is not ideal to have full set of courses, thesis work and actual work ongoing at the same time. Still I am proud that I accomplished to finish my studies.

All this would not have been possible without the support and help from a number of people. They have helped me in many ways from the coffee table conversations to the actual improvement tips for the thesis. Especially I would like to thank Mikko Karikytö and Ericsson for making the thesis project possible by providing the topic and the funding. Thanks to Jarmo Harju the examiner of this thesis as well for the great support and rapid responses to the emails. From Ericsson I would also like to thank my thesis supervisor Kennet Mattsson and the ISMS master Mikko Suomu for the extensive support and guidance you have given me throughout the project. Of course, thank you belongs to all Ericsson PSIRT members as well for the support in the tasks related to the thesis and the actual implementation of the ISMS.

I would also to thank my fiancée Miia, my mother Tarja for understanding and supporting me through these years. My dad Juha I would like to thank for the advices regarding the upcoming work career. I would also like to thank my friends Jarno, Jussi, Juuso V, Mikko L, my brother Mikko, Toni and especially Juuso Nänimäinen for the conversations and the support that has guided me to this point. Without you this would not have been possible.

Tampere, 07.05.2015

Lasse Laukka

TABLE OF CONTENTS

LIST OF ABBREVIATIONS AND SYMBOLS

3PP	Third Party Product
CERT	Computer Emergency Response Team
CERT-CC	Computer Emergency Response Team Coordination Center
COBIT	Control Objectives for Information and Related Technology
CSIRT	Computer Security Incident Response Team
CSRC	Computer Security Response Center
IEC	International Electrotechnical Commission
ISA	International Federation of the National Standardizing Associations
ISMS	Information Security Management System
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
JTC1	Joint Technical Committee that launched ISO 27001 standard
NCSC-FI	National Cyber Security Center Finland
PSIRT	Product Security Incident Response Team
RA	Risk assessment
SIM3	Security Incident Management Maturity Model
SoA	Statement of Applicability
UNSCC	United Nations Standards Coordinating Committee

1. INTRODUCTION

Information security is a concern when talking about managing information in organizations. Without securing organizational assets, processes and other information something will eventually go wrong. Securing informational assets will produce costs but in wider view it can result in savings. Integrity, Availability and Confidentiality are the key components that make an organization aware of the state of information security. Security is not something one can easily apply for organization. Security is about people, processes, assets and ways of working.

Information Security Management System (ISMS) is a framework that aims to fulfil these requirements by establishing new processes, developing existing processes and documenting valuable assets. ISO 27001 is an international standard that provides requirements for establishing, implementing, maintaining and continuously improving an information security management system and it is developed and maintained by ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) organizations [1]. ISO is one of the most influental standardization organizations of today and it is well known from quality management system standard ISO 9001 which is implemented by over one million companies and organizations in over 170 countries [13]. ISO 27001 was developed in the year 2005 [12] to meet organizational information security needs. It has been updated several times and as of today the latest version is ISO 27001:2013 [1].

The purpose of this thesis is to establish and implement an ISMS (Information Security Management System) for a CERT (Computer Emergency Response Team) by developing a suitable implementation process for the ISMS. In practice ISMS will be established for the Ericsson PSIRT (Product Security Incident Response Team) in Oy L M Ericsson AB. As ISMS requires continuous work this thesis will act as a starting point for the implementation of ISMS. Ericsson already has a global ISMS and parts that are excluded from the PSIRT ISMS will be covered by the global ISMS. On the other hand team level ISMS will ensure that the controls that are defined in the global ISMS will be in place.

In general CERTs are responsible for investigating security related incidents that

occur in the responsibility area of the team. Often these teams are responsible for proactive vulnerability management, incident co-ordination and reporting in their constituency. National CERTs monitor activities that can be dangerous to the society for example frauds that target to national banks. In telecom industry there are different kinds of CERTs. CERTs that work for operators are monitoring and scanning malicious activities in their network. Telecom vendors such as Ericsson are monitoring vulnerabilities and frauds that affect Ericsson products.

In Ericsson, PSIRT is responsible for Ericsson's product portfolio. PSIRT is not responsible for internal IT that Ericsson as a corporation has. PSIRT does vulnerability management as a service for Ericsson's product development units. PSIRT also helps with coordinating vulnerability incidents Ericsson wide. Ericsson has approximately 110 000 employees all over the world and PSIRT serves them all.

This thesis will go through different kinds of information security frameworks and the background of ISO 27000 standard family. It will explain the purpose of the Information Security Management system for organizations and then provide the guideline how to implement it to a CERT. A comparison between ISO 27000 standard family and SIM3 Security Incident Management Maturity Model is presented in this thesis as well. Finally there are conclusions of the whole implementation procedure in the end of this thesis.

2. COMPUTER EMERGENCY RESPONSE TEAM

Information security depends on humans, human activities, technical solutions and monitoring systems. It is not straightforward to maintain decired level of security. Information security work needs to be organized, monitored and constantly improved in order to achieve a good level within an organization. The only way to maintain a decent security level in an organization is to actively monitor, act and investigate security incidents and malicious behavior.

CERT - Computer Emergency Response Team is an organization that performs activities such as vulnerability coordination, scanning for new threats, informing different organizations or individuals of new threats and vulnerabilities. Having a CERT is a way to have a centralized capability for analyzing security events, coordinate incidents and ensure that information on these incidents and events is conveyed to those who need it [17].

2.1 Background

The acronym CERT (Computer Emergency Response Team) is used throughout this thesis. Other terms such as CSIRT (Computer Security Incident Response Team) or CSRC (Computer Security Response Centre) are also widely used [17]. The used name is often in relation to its constituency. For example vendors like Ericsson have PSIRT (Product Security Incident Response Team) and its constituency is Ericsson products. It is responsible for product security related incidents and vulnerability coordination of Ericsson products. It is a single contact point in all security issues that relate to Ericsson products but it is not responsible for corporate IT infrastructure or security incidents related to internal IT.

Nations often have their own CERT teams. In Finland there is NCSC-FI (National Cyber Security Center Finland) that is part of the Finnish Communications Regulatory Authority. It investigates security incidents that have an effect on the Finnish nation in larger scale. By actively monitoring Finnish networks in co-operation with

the Finnish operators, it publishes advisories for example when there is a phishing attack focused on Finnish banks. It also helps other authorities in investigating information technology related crimes.

2.2 Responsibilities

Computer Emergency Response Teams are the first point of contact when signs of malicious activity have been detected. CERT team is a contact point for security incidents. The responsibilities that a CERT team has are highly dependent on the constituency. If the team is an operator's CERT the responsibilities vary from network monitoring to analyzing and monitoring vulnerabilities.

Usually a CERT coordinates information security issues. If a new virus is spread in the network, CERT is the party that will act as a coordinator to keep track of activities, guidance information and other incident related data. It is up to the company management what type of responsibilities are after all assigned to a CERT. If organization is small the CERT might have several other security related duties in addition to the normal vulnerability analysis, coordination and monitoring. Sometimes a CERT might even have a regulative role within the organization by approving and monitoring security measures in place.

A CERT might also educate the rest of the organization by training other teams and being involved in organizational developing by emphasizing the importance of security. [17]

2.3 Ericsson PSIRT

This thesis was done for Ericsson PSIRT. ISMS implementation was started at the same time with this thesis work and as a result the ISMS was established for Ericsson PSIRT. PSIRT is responsible for the processes and procedures supporting product security in Ericsson worldwide. Internal IT infrastructure e.g. laptops, antivirus software or internal network design is not part of PSIRT's responsibilities.

As a vendor of critical infrastructure it is very important for Ericsson to have secure products delivered to the customers. PSIRT is part of the process of securing Ericsson's products. PSIRT monitors vulnerabilities published for the 3PP (Third Party Product) software that are in use in Ericsson products. For example if a vulnerability is published for a major Linux distribution, PSIRT will coordinate the actions for the product development units that have that specific Linux distribution in use in their product.

PSIRT also coordinates high and critical vulnerabilities in Ericsson. Due to wide use of certain 3pp components in products, a vulnerability in such component will affect multiple Ericsson products. Mitigation plans for all products are centrally monitored by Ericsson PSIRT.

Sometimes there are hundreds of products affected and they all need a mitigation plan. PSIRT acts as a single contact point in all product security matters in Ericsson.

3. INFORMATION SECURITY FRAMEWORKS

A number of different kinds of information security frameworks exist. They all have the same objective to raise the information security level of the target. Still they all do it in a different way. The advantage of ISO 27000 standard family is that it is a high level and complete set of documents that are needed in order to establish, implement and maintain an information security management system. There are a number of good criteria for evaluating IT systems but none of them is a complete solution for an organization to raise the security level and improve actions. Still most of these criteria documents can be useful while assessing the information security as an extensive set of controls is provided by them.

The upcoming sections will describe the most popular existing frameworks for improving information security or IT related operations.

3.1 TCSEC

Trusted Computer Security Evaluation Criteria (TCSEC) is a standard for evaluating the effectiveness of security controls which are part of the IT system products. TCSEC was developed by the United States Government Department of Defense (DoD) in 1983. TCSEC was later on in 2005 replaced by the Common Criteria (CC).

TCSEC was developed with three main principles in mind. It is designed to act as a yardstick for measuring the degree of trust in computer systems and it provides guidance for vendors when they are manufacturing trust based equipment. TCSEC also provides the basis for security requirements in acquisition specifications. [7]

TCSEC is not a tool for establishing ISMS but its controls might be useful for it.

3.2 ITSEC

Information Technology Security Evaluation Criteria (ITSEC) is an evaluation criteria for IT systems and IT products. By following this criteria end user is able to

evaluate IT systems and products. ITSEC was developed by the Commission of the European Communities in 1991.

ITSEC defines evaluation levels of confidence for the target of evaluation. These levels differ from E0 to E6. In order to get more specific evaluation more examination is needed. ITSEC is very similar to the DoD based TCSEC but the difference between them is that ITSEC is not functionality dependent. The evaluation levels can be assigned for example when the product is offering confidentiality features but not integrity. With TCSEC that is not possible.

In order to get ITSEC comparable with TCSEC, functionality classes are defined. With these functionality classes these two evaluation criteria are made comparable. [8]

As ITSEC is similar to TCSEC it will not help the organization to establish ISMS. Some of the controls might still be useful.

3.3 Common Criteria

Common Criteria is today's version of TCSEC evaluation criteria for the security features in IT products. Evaluation process according to Common Criteria establishes a level of confidence that the IT products meet these requirements. The point of the criteria is to provide a tool to compare different solutions or products to each other from the security perspective.

Common Criteria has very different purpose and it is not really helping in the process of implementing an ISMS. Still it provides very extensive set of tools to evaluate security functionalities. [6]

3.4 COBIT

Control Objectives for Information and Related Technology (COBIT) is a framework that is designed to control the whole IT environment in an organization. It is a toolset for IT management and governance. It is not an information security framework but it has some similarities to ISO 27000 standard family. For example it includes risk management as a part of the framework.

The focus of the COBIT framework is to meet the business requirements set to the IT of an organization. In this thesis we will concentrate to the management of information security so COBIT is not an ideal framework for that use case.

3.5 ITIL

Information Technology Infrastructure Library (ITIL) is a framework which consists of a set of best practices for IT service management. It is a widely used framework but the scope of this framework is to provide guidance for organizations to recognize the IT resources and services as business assets. ITIL concentrates on planning IT and business strategies and the primary objective is to make sure that the IT services are aligned with the business needs.

In terms of the ISMS ITIL does not offer too much. ITIL can be used in conjunction with other frameworks but itself it does not fulfill any ISMS needs. [10]

3.6 SIM3: Security Incident Management Maturity Model

SIM3 Security Incident Management Maturity Model is a document that is used to evaluate the maturity of a CERT. It is developed by Don Stiikvort and is used as a reference model for Trusted Introducer accredidation. The SIM3 model covers four major areas of the CERT operations which are prevention, detection, resolution, and quality control and feedback. [23]

The actual evaluation is done via three basic elements. The elements are maturity parameters, quadrants and levels. There are more than 40 different maturity parameters in the model and each of them belongs to a certain quadrant. After the evaluation each parameter will be assigned with a value which is called level in the model. Maturity quadrants and the maturity levels are presented in Table 3.1

Maturity Quadrants	**Maturity Levels**
O - Organization	0 = not available
H - Human	1 = implicit
T - Tools	2 = explicit, internal
P - Processes	3 = explicit, formalised on authority of CSIRT head
	4 = explicit, audited on authority of governance levels above the CSIRT head

Table 3.1 *Maturity quadrants and levels of the SIM3 model [23]*

The maturity quadrants provide a top level view to what topics the SIM3 model concentrates. It covers aspects from organization, human, tool and processes point of views. Each of the quadrants have about 10 parameters which are rated during the evaluation with the values from 0 to 4. The levels are also explained in more readable wording as presented in Table 3.2.

Maturity level	explanation
0 = not available	undefined / unaware
1 = implicit	Known or considered but not in a written form.
2 = explicit, internal	Written but not formalised by for example the head of CERT
3 = explicit, formalised	Written and authorized by an authority
4 = explicit, audited on authority	Audited above CERT head

Table 3.2 *Maturity level descriptions [23]*

Even though the parameters have been developed in a long term process and throughout several years the basis of is not the ISO 27001. However the security objectives from the ISO 27001 cover most of the quadrants and parameters of the SIM3 as will be discussed in the next chapter (in Section 4.5).

SIM3 is a great way to measure the maturity of a CERT. However the minimum requirements for the parameters are not presented in the model itself. The requirements for the maturity are therefore in the hands of the executing organization. Trusted Introducer, which is a one of the top organizations for CERT teams, uses a set of requirements for SIM3 parameters for accredidation and that is a good starting point for defining the correct level of maturity in the target organization.

SIM3 is a great model and it can be used in addition to ISMS. It is one way for assessing the effectiveness and the suitability of the ISMS for a CERT. A comparison between SIM3 and ISO 27000 standard family is presented in Section 4.5.

3.7 ISO 27000

ISO 27000 is the de facto standard family in order to establish, implement and maintain an ISMS. ISO 27000 is used among different kinds of organizations worldwide and it provides an extensive set of tools and documents for the purpose. ISO 27000 will be covered in the next section of this thesis.

4. ISO 27000 STANDARD FAMILY

ISO 27000 is a risk based standard family that is designed to be used as a reference when developing an Information Security Management System. It is intended to work with all types and sizes of organizations. As a whole it defines how to implement an ISMS properly. Once the ISMS has been implemented an organization will gain a holistic and coordinated view of the security risks, state of information security and the ways to improve.

ISO 27000 standard consists of several documents. ISO 27001 defines the requirements for implementing an ISMS, ISO 27002 will have a general overview over the ISO 27001 controls followed by the implementation guidance for each control. [1] [2]. ISO 27003 will help in developing an implementation plan for ISMS and gives concrete examples and ideas how to do that. [3]. ISO 27005 is a risk management standard that is designed to help in the implementation of information security from a risk management point of view. ISO 27005 supports the general concepts represented in ISO 27001 [5].

4.1 History of the International Organization for Standardization

In 14 to 26 October 1946 65 delegates from 25 countries came to London to plan the future of international standardization. In that conference ISO (International Organization for standardization) was established and later born from the union of ISA (International Federation of the National Standardizing Associations) and UNSCC (United Nations Standards Coordinating Committee). [12] [18].

In 1947 ISO set up 67 technical committees and most of them were formerly belonged to ISA. After that ISO has produced a number of internationally recognized standards. The ISO 9000 quality management standard family is the best known of them all.

As information security raised its head as one of the most important factor in business world, ISO's and IEC's joint committee introduced ISO 27001 Information

Security Management System standard in 2005. Organizations worldwide have been implementing this standard to gain satisfying level of information security. ISO 27001 is a framework that provides tools for establishing, implementing and maintaining processes, controls and required documents for information security needs. As of today the ISO 27001 is one of the most popular standards among the ISO 9000 standard family [12] [18].

4.2 ISO 27001

ISO 27001 was launched in 2005 by ISO and IEC's joint technical committee JTC1 [12]. ISO 27001 standard provides risk based requirements for establishing, implementing, maintaining and continually improving an information security management system, ISMS [1]. The purpose of ISMS is to provide tools, processes and ways of working to improve the level of information security.

The requirements consist of control objectives and the actual controls which represent the plausible risks and the mitigation for each risk. ISO27001 itself is a good starting point when developing information security. It is also a vital document in the actual implementation phase when selecting appropriate controls on the risks identified in the risk assessment. The new version of the standard ISO27001:2013 does not strictly define that the controls must be selected from it. Controls in the overall implementation can be also selected from other sources such as other best practices [1].

ISO 27001 consists of the actual requirement part and the Annex A. The requirement part does not contain the actual controls but it defines the areas to be assessed. Annex A however is the part with all the security controls.

The requirement part contains seven different areas which are The Context of the Organization, Leadership, Planning, Support, Operation, Performance Evaluation and Improvement. These are the areas that need to be addressed during the implementation of the ISMS.

Requirements for each of the seven areas are shortly explained. There are only a few points in each area and these points are written in very general way. There are no practical examples or advices on how to actually implement each of the areas. Practical implementation guidance is however presented in ISO 27002 but still in order to implement and be compliant to the ISO 27001 standard it requires a lot of resources, time and effort to tailor the areas of the standard to each organization.

Annex A has been divided to control objectives and the actual controls which are

related to the specific control objective. These control objectives fulfil the requirements that have been set by the actual requirement part of the document. There is no direct link between the controls and the requirement areas but by assessing risks related to each control objective the organization is capable of implementing the standard successfully.

4.3 ISO 27002

ISO 27002 is a guideline for implementing best practices of information security. It gives information about implementation, selection and management of controls from ISO 27001. ISO 27002 consists of three key areas: selection of controls from ISO 27001, implementation of the controls, and finally, instructions on developing own information security management guidelines.

With ISO 27001 and ISO 27002 documents an organization should be able to identify risks, select appropriate controls and implement those controls. With the help of ISO 27002 an organization is also able to produce the documents needed in terms of the standard but also in terms of improving and developing a working ISMS.

ISO 27002 categorization follows the same structure as the ISO 27001. Control objectives from ISO 27001 are called clauses in ISO 27002. A description and practical advice for every clause and every control within that clause is provided.

The problem with this guidance is that if a risk in the organization has been identified, there might not be any control that would specifically mitigate the issue in the target organization. Organization should then develop their own control for mitigating that risk. ISO 27002 might still be useful and it can provide input for the risk assessment itself as well. It can also act as a steering document for the asset identification and risk assessment. The target organization should review all the control objectives from ISO 27001 and ISO 27002 in order to have full governance of the assets related to information security.

In this thesis the problem of the control selection approach in risk treatment has been dealt with by turning the process other way around. A risk treatment plan will be made by determining proper actions for mitigating the identified risks and then selecting corresponding control objectives and controls from the standard to represent the compliance for the standard.

4.4 ISO 27005

ISO 27005 is a standard that is designed to support ISO 27001 and ISO 27002. ISO 27005 consist of guidelines for information security risk management. [5] This standard covers the risk assessment process that will help organizations to successfully implement ISMS.

According to the ISO 27005, risk assessment can be divided into three main phases: risk identification, risk analysis and risk evaluation. After the risk assessment risk treatment is applied for the identified, analyzed and evaluated risks in order to mitigate and lower the impact of the risks. With the help of ISO 27005 the organization is able to conduct the most vital part, the risk assessment, of the ISMS.

4.5 Comparison between SIM3 model and ISO 27000 standard family

As there are similarities between the SIM3 Security Incident Management Maturity Model and the ISO 27000 standard family, a comparison was done as a part of this thesis. The basis of the SIM3 model are the processes and ways of working that a CERT needs to have in order to gain maturity in its own constituency. The approach is different to ISO 27000 standard family which is a general standard meant for every organization.

However these two models have a lot of similarities and a correlation between some of the parameters and the control objectives from ISO 27001 can be found. Of course all of them are not fully or even partly correspondent to each other as Tables 4.1, 4.2, 4.3 and 4.4 show.

In this comparison the basis was to have the SIM3 parameters as a reference and a mapping to correspondent security control objective from the ISO 27001 standard was done.

Maturity quadrant: Organizational

SIM3 Parameter **Maturity quadrant: Organizational**	**ISO 27001 Control Objective or Clause**
O-1 Mandate	A.5.1 Management direction for information security
O-2 Constituency	4.3 Determining the scope of the ISMS
O-3 Authority	A.5.1 Management direction for information security
O-4 Responsibility	A6.1 Internal organization
O-5 Service description	Not defined in ISO 27001. Could be part of the scope of the ISMS
O-6 Blank	Left blank intentionally in SIM3 [23]
O-7 Service level description	Not defined in ISO 27001.
O-8 Incident classification	A.16.1 Management of information security incidents and improvements
O-9 Integration in existing CSIRT systems	A.6.1 Internal organization: A.6.1.4 Contact with with special interest groups
O-10 Organizational framework	Not specifically included in ISO 27001. This parameter in SIM3 servers a different purpose. ISMS as a whole is similar to this parameter.
O-11 Security policy	A.5.1 Management direction for information security. More specifically the control A.5.1.1

Table 4.1 *Comparison of SIM3 Organizational parameters and ISO 27001 control objectives. [23], [1]*

As can be seen from Table 4.1 the ISO 27001 almost covers all the organizational parameters from the SIM3. O-5 and O-7 parameters, service description and service level description are not requirements in the ISO 27000 which is understandable because the ISO 27001 is concentrated to information security management. It does not cover any other managemental issues.

Maturity quadrant: Human

SIM3 Parameter Maturity quadrant: Human	**ISO 27001 Control Objective or Clause**
H-1 Code of conduct/practice/ethics	A.7.2 During employment. ISO 27001 defines only the responsibilities and disciplinary processes around information security breaches. It does not mention any code of ethics especially for private life.
H-2 Personal resilience	Corresponding control does not exist.
H-3 Skillset description	A.7.1.1 Screening and 7.2 Competence.
H-4 Internal training	7.2 Competence. It is not fully corresponding in terms of SIM3 requires internal trainings to be available where ISO 27001 requires personell to have sufficient training or competence.
H-5 External technical training	7.2 Competence. It is not fully corresponding.
H-6 Extrenal communication training	Corresponding control does not exist.
H-7 External networking	Corresponding control does not exist.

Table 4.2 *Comparison of SIM3 Human parameters and ISO 27001 control objectives. [23], [1]*

The difference between human parameters of the SIM3 and the ISO 27001 control objectives is more obvious. SIM3 provides accurate parameters for measuring the maturity of a CERT from human aspect. ISO 27001 does not require for example personal resilience as SIM3 does. For a CERT it is very important to have such policies and requirements. Still some of the parameters are partly correlating with the ISO 27001 security objectives.

Maturity quadrant: Tools

SIM3 Parameter Maturity quadrant: Tools and Processes	**ISO 27001 Control Objective**
T-1 IT Resources list	A.8 Asset management: A.8.1.1 Inventory of assets. In SIM3 the focus is more in the IT resource list of CERT's constituency. ISO 27001 focuses on internal assets.
T-2 Information sources list	Corresponding control does not exist.
T-3 Consolidated e-mail system	Corresponding control does not exist.
T-4 Incident tracking system	Corresponding control does not exist. ISO 27001 mainly focuses on the security of the computer systems. For example control A.12.5 Control of operational software will ensure the integrity of operational systems.
T-5 Resilient phone	Corresponding control does not exist.
T-6 Resilient e-mail	Corresponding control does not exist.
T-7 Resilient internet access	Corresponding control does not exist.
T-8 Incident prevention toolset	Corresponding control does not exist.
T-9 Incident detection toolset	Corresponding control does not exist.
T-10 Incident resolution toolset	Corresponding control does not exist.

Table 4.3 *Comparison of SIM3 Tools parameters and ISO 27001 control objectives. [23], [1]*

The SIM3 tools and processes parameter list is targeted to cover the IT system aspect of the CERT's maturity. Most of the parameters do not map with the ISO 27001 at all. This is because ISO 27001 does not give any specific recommendations or requirements for specific organizations.

SIM3 goes to a very practical level with the parameters from T-5 to T-10. Resilient phone, e-mail and internet access are very important in the context of a CERT. For ISO standard it is not relevant information.

Maturity quadrant: Processes

The parameter list for processes has some correlation with the ISO 27001. Escalation paths, incident management processes and information handling processes are

SIM3 Parameter Maturity quadrant: Processes	**ISO 27001 Control Objective**
P-1 Escalation to governance level	A.16.1 Management of information security incidents and improvements. A.16.1.2 Reporting information security events. 7.4 Communication. SIM3 provides more practical parameters for this purpose. ISO 27001 controls are very general.
P-2 Escalation to press function	A.16.1 especially A.16.1.2, 7.4 Communication
P-3 Escalation to legal function	A.16.1 especially A.16.1.2, 7.4 Communication
P-4 Incident prevention process	Corresponding control does not exist. Partly A.16 as a whole.
P-5 Incident detection process	Corresponding control does not exist. Partly A.16 as a whole.
P-6 Incident resolution process	A.16.1.4, A.16.1.5, A.16.1.6
P-7 Specific incident processes	Corresponding control does not exist.
P-8 Audit / feedback process	A.17.1, A.17.1.3, A.18.2
P-9 Emergency reachability process	Corresponding control does not exist.
P-10 Best practice e-mail and web presence	Corresponding control does not exist.
P-11 Secure information handling process	A.8.3, A.13.2, A.18,
P-12 Information sources process	Corresponding control does not exist.
P-13 Outreach process	Corresponding control does not exist.
P-14 Reporting process	Corresponding control does not exist.
P-15 Statistics process	Corresponding control does not exist.
P-16 Meeting process	Corresponding control does not exist.
P-17 Peer-to-peer process	Corresponding control does not exist.

Table 4.4 *Comparison of SIM3 Processes parameters and ISO 27001 control objectives. [23], [1]*

correlating with each other in SIM3 and ISO 27001. Again SIM3 offers more practical view of the processes but a lot of similarities are found. Suprisingly the ISO 27001 does not mention any requirements on the reporting or statistics processes. ISO 27001 has a clause for monitoring and measuring the performance of the ISMS but it is not what the SIM3 model is after.

Summary of the comparison

The SIM3 Security Incident Management Maturity Model provides a set of parametesr for measuring the maturity of a CERT. These parameters are divided into four different quadrants and they will cover all the critical aspects that are needed

to have properly functioning and effective CERT. SIM3 provides practical examples of the parameters and by analyzing those parameters the CERT is able to develop the effectiveness, information security level and reachability.

The SIM3 Security Incident Management Maturity Model is not based on the ISO 27000 standard family. That can be seen from the comparison and the correlation between ISO 27001 security objectives and the SIM3 parameters. Still some of the parameters will have a strong correlation but most of them not.

From the ISMS point of view the most important thing is that the SIM3 is defining the areas that a CERT needs to concetrate when developing the maturity of the team. It would be highly recommended to use SIM3 parameters as additional controls in the ISMS. By combining the ISMS and the SIM3 model it is possible to reach a very high maturity level in a CERT. The ISO 27001 will provide the basis for the ISMS and the SIM3 will complete the control set from CERT aspect. SIM3 model is also a good example how much tailoring the ISO 27001 needs when one wants to implement the ISMS for a CERT. ISO 27001 is not a complete package for a CERT.

5. ISMS IMPLEMENTATION PROCESS

There are numerous ways to implement ISO 27001 standard. The steps needed are highly dependent on the target organization. In this thesis the target organization is a CERT. The implementation steps presented in this chapter are seen the most suitable for a CERT team by Ericsson PSIRT. The formula for the implementation process was developed while assessing risks for Ericsson PSIRT. Certification phase is intentionally excluded from the scope of this thesis because Ericsson PSIRT will not acquire ISO 27001 certificate. This thesis uses ISO 27001:2013 standard as a basis for the ISMS implementation.

ISMS requires certain documentation. This documentation forms the actual ISMS and is the most essential part of it. The documents in ISMS have to be properly controlled and protected. Organization has to define a procedure for controlling the documents within the ISMS. All required documents are presented in Table 5.1 and 5.2 [1]

Document name	**Clause in ISO 27001:2013**
The scope of the ISMS	4.3
Information security policy and objectives	5.2, 6.2
Risk assessment and risk treatment methodology	6.1.2
Statement of Applicability	6.1.3d
A risk treatment plan	6.1.3e, 6.2
Risk assessment report	8.2
Definition of security roles and responsibilities	A.7.1.2, A.13.2.4
Inventory of assets	A.8.1.1
Acceptable use of assets	A.8.1.3
Access control policy	A.9.1.1
Operating procedures for IT management	A.12.1.1
Secure system engineering principles	A.14.2.5
Supplier security policy	A.15.1.1
Incident management procedure	A.16.1.5
Business continuity procedures	A.17.1.2
Legal, regulatory, and contractual requirements	A.18.1.1

Table 5.1 *List of minimum set of mandatory documents required by the ISO 27001:2013 [1], [20]*

Document name	Clause in ISO 27001:2013
Records of training, skills, experience and qualifications	7.2
Monitoring and measurement results	9.1
Internal audit program	9.2
Results of internal audits	9.2
Results of the management review	9.3
Results of corrective actions	10.1
Logs of user activities, exceptions, and security events	A.12.4.2, A12.4.3

Table 5.2 *List of minimum set of mandatory records required by the ISO 27001:2013 [1], [20]*

These documents have to exist in the ISMS. Otherwise the organization cannot be compliant to the standard. The amount of required documents has increased from the previous version of the standard ISO 27001:2005. At the same time the freedom for choosing the controls has increased. This causes difficulties for the implementation because now the requirements are looser.

Implementation process of this thesis consists of three main phases, establishment, implementation and continuous improvement. Figure 5.1 illustrates these phases and tasks in each phase. This implementation process description can be used as a starting point when implementing an ISMS for a CERT.

General ISMS implementation guidelines exist but this thesis represents a guideline specifically tailored for a CERT. It concentrates on the key issues faced by a CERT in terms of information security. Following the guidelines given in this thesis a CERT is able to establish an ISMS efficiently.

5.1 Establishment

The first of the three main phases is establishment. During the establishment the scope will be determined, assets will be listed, risks are assessed and the proper risk treatment and controls to mitigate the risks will be chosen. In this phase most of the documents required by the ISO 27001:2013 standard will be created. Establishment sets the basis for the ISMS.

5.1.1 Management commitment

According to the ISO 27001 standard the establishment of an ISMS starts with the commitment of organization management. To start the implementation of information security management system, organization management has to commit to it

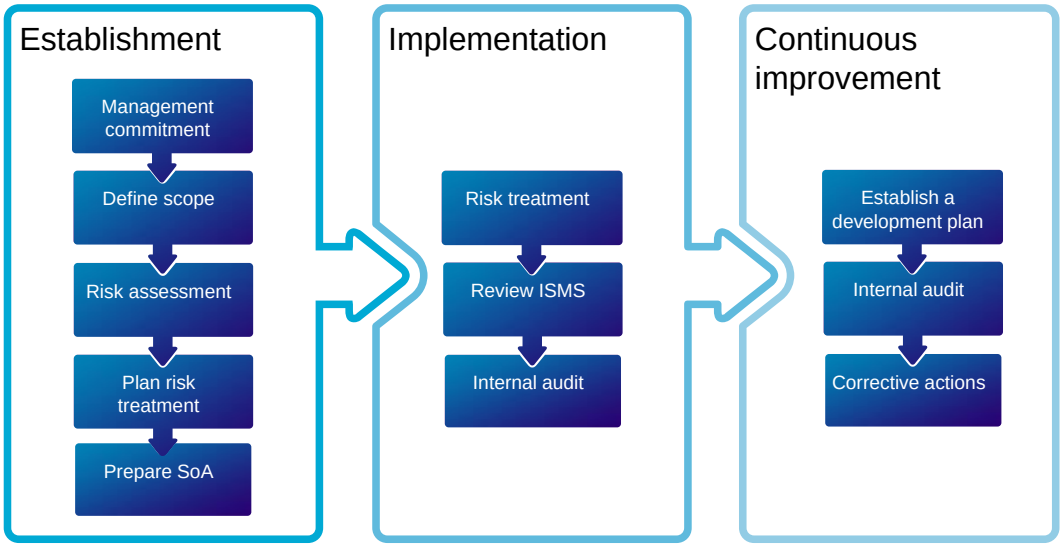

Figure 5.1 *ISMS implementation process description for Ericsson PSIRT*

by allocating relevant resources, people, time and funding. Top management should demonstrate the commitment by ensuring that the information security policies and objectives have been established and that the integration of the ISMS requirements into the organization's processes is possible [1].

Top management should encourage and lead supporting persons to make an effort in the ISMS and promote the continuous improvement of information security management system. This commitment should be documented and communicated throughout the target organization. [1] [14]

The essential part of the management commitment is to establish an ISMS organization within the target organization. That means that in order to make the ISMS effective and ensure that the continuous improvement will be followed, responsible people have to be nominated. The key person to be chosen is the ISMS manager who ensures the compliance by maintaining and monitoring the execution of the processes of ISMS. ISMS also needs a steering group which usually is formed from the stakeholders of the team. Steering group will provide the funding for the project but also benefit from the improvements the ISMS does for the organization's informa-

tion security. As a result a document defining the security roles and responsibilities will be created.

The requirement for this document can be found from the ISO 27001 controls A7.1.2 and A.13.2.4. The standard only requires confidentiality or non-disclosure agreements and the rules how the target organization staff can handle information. It does not define that there is a need for a separate ISMS organization to steer the project. However the establishment of an ISMS organization has been seen very useful in the practice with Ericsson PSIRT. It will also ensure the continuity of the ISMS tasks in the future. The ISMS organization can be a virtual organization but depending on the scope of the ISMS a separate full time organization can be formed.

5.1.2 Define scope

When the management commitment has been obtained the scope of the ISMS will be defined. The scope has to be tailored for the target organization and it is very dependent on the nature of the target. Organization should recognize and document processes and areas that ISMS should have an effect on. If the organization is part of a bigger organization the scope should cover the functions of this specific team, and exclude the parts that will be covered through the higher level policies and possible ISMS. If something is excluded, the exception should be documented and explained thoroughly. [19].

The definition of the scope has to include a description of the target organization, business functions, business processes, assets and everything that can have impact on the information security. It is important to gain knowledge about the whole environment of the target organization. What does it do, what are the parties it is in communication with, are there existing security controls in place? [19] [1]

In the case of CERT the scope should cover all critical and important assets, processes, tools, physical access and the ways of working that have an effect on the existence, functions and business continuity of the team. As a CERT is offering information security services for its constituency it is very important that the internal information security is managed and improved by the best practices. As a CERT executes very agile and time-critical functions the risks that have impact on availability will have a significant role.

ISO 27001:2013 requires that the scope of the ISMS has to be documented. The document should be signed to indicate the management commitment and support for ISMS.

Create and define ISMS policy

ISMS policy is a document that contains the final boundaries and objectives for the whole information security management system. The policy must serve the purpose of the organization and include information security objectives related to the target organization. If no objectives are set in the policy, framework to meet these objectives has to be established. [1]

The ISMS policy is the basis of the ISMS documentation. Therefore it has to be approved and signed by the top management of the organization. ISMS policy also contains the documentation of the ISMS organization roles and responsibilities. It should contain information on how the organization will execute, maintain and improve the ISMS. ISMS policy has to be communicated within the organization and a commitment to follow to policy has to be obtained from all organization members [1].

5.1.3 Risk assessment

ISO 27000 is a risk based information security framework. Therefore risk assessment is the foundation of the whole system. By identifying, analyzing and treating the risks in an efficient way, an organization is able to take full advantage of the ISMS.

Risks must be addressed because the confidentiality, integrity and availability of assets can be essential part of the operations of the organization. If some of these three key attributes of information security is broken it can be hard to maintain cash flow, profitability, competitive edge or legal compliance. Also the image and brand of an organization may suffer from the information security incident. [22]

The risk assessment method to be used is not defined in the ISO 27001 standard and therefore the target organization has to choose a suitable method for assessing the risks. The method used should cover all control areas defined in the standard e.g. procedures and processes, legal, regulatory matters and personnel. The methodology chosen should be documented to the risk assessment and treatment methodology document. If risk treatment methodology is not decided in this step, the document produced can remain in the draft state and be updated with the risk treatment information when created. [22]

For this thesis risks are assessed according to the risk management process of ISO 27005 standard. It is an extensive and widely used standard for identifying, analyzing, evaluating and, after all, managing risks. The risks management process is

presented in Figure 5.2. Before continuing to the first phase of risk assessment the risk management process has to be established. It will support the ISMS and will act as a reference point later on in the risk assessment phase. Risk evaluation criteria, impact criteria and risk acceptance criteria have to be created. [4]

As a result from the risk assessment step risk assessment and methodology, risk assessment report and risk treatment plan will be created.

Risk identification

The purpose of risk identification is to find out what could lead to a potential loss and to gather information on how to prevent these occurrences. [4] Risk identification starts with the identification of assets. Without knowledge over organizational assets it is hard to execute effective risk assessment. All risks are bound to the assets in this ISMS implementation.

To successfully identify all organizational assets the people in the organization has to work together. A workshop is a good idea to discuss and define all assets. The ISMS scope definition can also act as input for the asset recognition [14]. An organization should identify all valuable items and their relations with each other for the risk assessment. If asset identification is improperly done, the risk assessment will not have sufficient input and the effectiveness of the ISMS will suffer. If there are enough resources available, multiple workshops can be held to get a deeper view on the assets. It is common that not all things come to mind at first and therefore it is recommended to have multiple workshops. Identified assets should be organized and ranked by their nature and value. An owner should be assigned for each asset.

All assets should be documented to ISMS. This document is a mandatory part of ISO 27001 requirements and the document should be named as Inventory of Assets. This list should be updated during every round in continuous improvement phase. In the inventory of assets document the importance and owner for each asset should be defined. This will act as input for the actual risk identification. A policy how listed assets can be used has to be created. As an output a document called Acceptable Use of Assets will be created and stored to the ISMS.

Risk identification itself is based on the asset identification. In the risk identification workshop all assets are reviewed and risks for each asset are recognized. These risks are analyzed in the risk analysis part.

Risk evaluation criteria

Risk evaluation criteria will be created at this stage of the implementation. It is important to have reference criteria ready when executing the risk assessment. The evaluation criteria should be created considering the criticality of the information assets identified in the previous step. The evaluation criteria should also reflect the expectations of stakeholders, regulatory and legal obligations. [4]

Risk assessment results will be compared against the risk evaluation criteria to prioritize the risks for risk treatment. If no criteria exists it is very hard to gain a holistic view of the severity of risks. Risk evaluation criteria can be also used as a reference point when choosing the sufficient scale for risks. It acts as an input for the risk acceptance criteria as well. [4]

Risk evaluation criteria will be part of the risk assessment and methodology document in the ISMS.

Risk acceptance criteria

In order to gain knowledge over what is a serious risk and what is low risk appropriate criteria have to be defined. Risk acceptance criteria will define whether a risk can be accepted as it is and no risk treatment will be applied for it. The basis of the risk acceptance criteria is that if a risk cost is lower than the mitigation cost, risk can be accepted.

Every organization has to specify their own risk acceptance scales. The interests of the stakeholder, organization's policies and strategy as well as regulatory requirements can influence the acceptance levels. [4].

Every risk has to be analyzed carefully and a decision whether to mitigate or accept it has to be made. Risk acceptance criteria should be documented to the risk assessment and methodology document in the ISMS.

Figure 5.2 represents the whole risk managing process but the part that is needed for ISMS risk assessment is marked with the dotted line. The actual risk assessment consists of risk identification, risk analysis and risk evaluation. Risk treatment is also part of ISMS but it will be covered in the implementation phase.

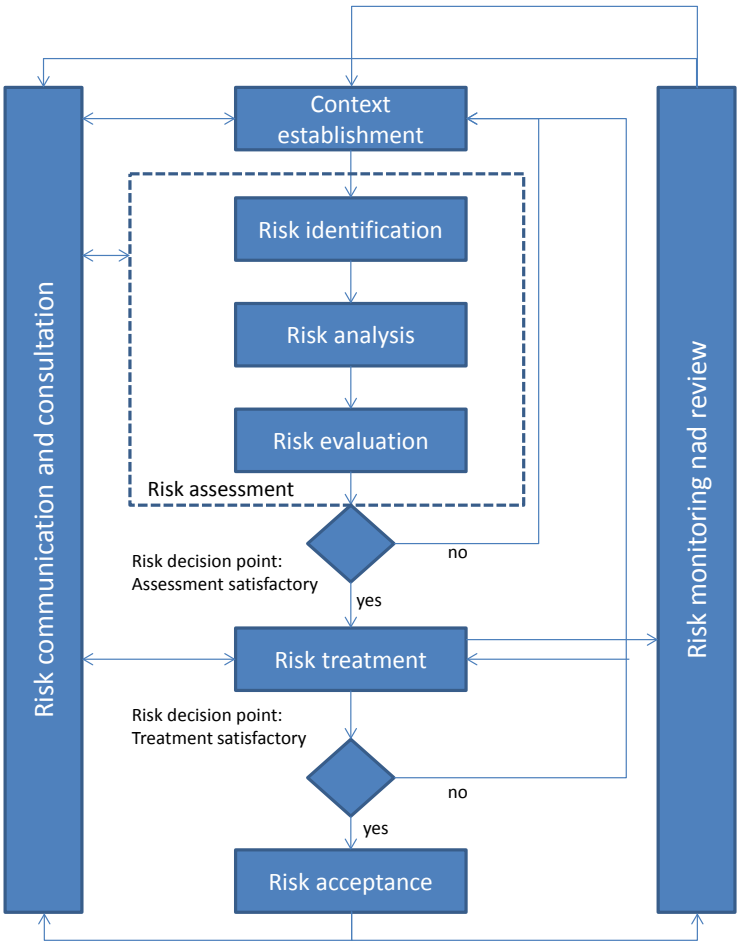

Figure 5.2 *Risk management process according to ISO 27005:2011 [4]*

Risk analysis

After identification of risks another workshop has to be arranged. In this workshop or series of workshops all risks identified are evaluated and rated according to the criteria defined in risk assessment and risk treatment methodology document of the ISMS.

As described in the ISO 27005 standard risk analysis can be qualitative or quantitative. As a CERT is a team and commonly the risks related to it cannot be measured with numbers a qualitative analysis is a better choice. The aim of qualitative analysis is to describe the business impact and the probability of the occurrence by defining a scale for example with values Low, Medium, High and setting a reasonable and

real life bonding probability scale based on the experience of the organization.

The advantage of the qualitative analysis is to provide very understandable formatting to all risks and the impact of each risk is easy to understand. On the other hand this method is vulnerable to misinterpretation of the scale. How to rate a specific risk as low? That is very important and subjective choice of the scale and has to be analyzed carefully by the ISMS organization. [4]

Each risk identified in the previous step will be assessed by the means of consequences and likelihood. A risk level will be determined from these two scales. As a result of the risk analysis phase the organization has a list of all identified risks rated with a comparable risk level value. Risk level matrix is presented in Figure 5.3. The overall value gained from the matrix will define the level of risk. Low risk will have a value between 0-2, medium risk 3-5 and a high risk 6-8. [4]

	Likelihood of incident scenario	Very Low	Low	Medium	High	Very High
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

Figure 5.3 *Risk level matrix [4]*

Risk evaluation

After assigning the risk level values for all risks, these values have to be compared to the risk evaluation and risk acceptance criteria. The risk evaluation will offer input to make the decision over the risk treatment and whether risks should be addressed or not. Risk treatment has to be made with cost efficiency in mind. If the cost of the mitigation is more than the value of the realized risk, there is no point in mitigating.

The purpose of the risk evaluation stage is to make decision over the risks. One important step in this stage is to evaluate the contractual, legal and regulatory requirements that are in relation to a specific risk. That is one factor to decide whether the risk should be mitigated or accepted.

Risk evaluation also provides a tool to prioritize risks for risk treatment. Usually not every risk can be treated at once so prioritization has to be done. As an output the organization will gain a list of rated risks with a prioritized order for control selection.

5.1.4 Plan the risk treatment

ISO 27000 standard defines a set of controls that can be used as a reference when mitigating the risks identified during the risk assessment. A control is an example of the risk and the mitigation plan for that specific risk. As the set of controls in the ISO 27001 is extensive, there are lots of solutions for different kinds of organizations.

Risk treatment will be applied for each risk identified and analyzed during the risk assessment. With the implementation of specific control for specific risk the organization is able to mitigate or lower the impact of the risk. Risk treatment can be planned from the standard perspective by going through the controls of the standard and developing and updating the processes and ways of working accordingly. If all risks are not mitigated during this procedure, controls from other sources are needed.

More effective way to is to take a risk based approach when planning the risk treatment. Analyzing the risks assessed and determining a mitigation for each risk separately without binding the treaments strictly to the controls of the standard. The mitigations for risks can be compared to the controls of the standard afterwards to represent the compliance to the standard. By planning the risk treatment this way the organization is able to concentrate more on the actual mitigations rather than focusing on the whole list of controls of the standard. Cost efficiency should not be forgotten when planning the risk treatment. When the risk treatment for each risk has been found, the controls from the standard have to be analyzed. The controls of the ISO 27001 can then act as input for the risk treatment and therefore it is possible to also identify new risks through that.

The most important thing regardless of the way how that is achieved is to mitigate the identified risks. In order to be compliant to the standard, all control objectives and controls have to be evaluated and taken into use if necessary.

In the earlier revisions of the ISO 27001 standard there were no options to select controls anywhere else but from the standard itself. Now ISO 27001:2013 gives the opportunity to select controls from various sources. Controls can be implemented from the best practices or anywhere else if they are considered useful. ISO 27001 still offers an extensive set of controls.

If control areas or controls are excluded from the ISMS, these exceptions should be documented and justified with adequate explanation.

Risk treatment plan should be done with cost efficiency in mind. If the cost of the implementation of the control exceeds the cost of the realized risk there is no point to apply that control to the risk. A decision whether the risk should be mitigated or accepted have to be done before applying any controls over it.

Risk treatment plan should be documented to the ISMS and it should demonstrate actions that needs to be taken to mitigate the risk. It should also state the owner for each risk, dependencies to other systems or risks if existing. Estimated completion time and the status should be also documented in the plan.

5.1.5 Statement of Applicability

When the risks have been assessed and the risk treatment plan have been created a SoA (Statement of Applicability) have to be created and documented to the ISMS. SoA will describe the current level of the implementation and continuous improvement process of ISO 27001. It states towards the standard what controls are in place, what are missing and which controls will not be included in the process. If controls from other sources are implemented that has to be stated in the SoA. SoA should be updated and it should always represent the current state of the ISMS. [21]

The SoA is a mandatory document. A listing of the control objectives and controls is not a valid SoA alone. A linkage between why a specific control has been selected for a specific risk has to be defined in the SoA. There are a lot of tools available for creating a SoA. One of the most useful and the most simple tool is an excel document with valid fields to satisfy the requirements of the SoA.

SoA should include all control objectives and controls from the standard. In addition the implementation status for each control objective and control should be there. A clear naming for the status has to be created. A four stage scale can be used for example: not applicable, not implemented, partially implemented, fully implemented. When all the controls are evaluated, a summary of the ISMS status can be made. In the summary the compliance for each control objective are presented. Example of the SoA summary is presented in Figure 5.4

	Section	COMPLIANCE	Not Applicable	Not Implemented	Partially Implemented	Fully Implemented
A5	SECURITY POLICY	100%	0	0	0	1
A6	ORGANIZATION OF INFORMATION SECURITY	25%	0	1	1	0
A7	HUMAN RESOURCE SECURITY	50%	0	1	1	1
A8	ASSET MANAGEMENT	50%	1	1	0	1
A9	ACCESS CONTROL	38%	0	2	1	1
A10	CRYPTOGRAPHY	50%	0	0	1	0
A11	PHYSICAL AND ENVIRONMENTAL SECURITY	100%	1	0	0	1
A12	OPERATIONS SECURITY	100%	0	0	0	7
A13	COMMUNICATIONS SECURITY	75%	0	0	1	1
A14	SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE	33%	0	1	2	0
A15	SUPPLIER RELATIONSHIPS	25%	0	1	1	0
A16	INFORMATION SECURITY INCIDENT MANAGEMENT	50%	0	0	1	0
A17	INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUIT	50%	0	1	0	1
A18	COMPLIANCE	25%	0	1	1	0

Figure 5.4 *Example of the statement of applicability summary*

5.2 Implementation

After ISMS has been successfully established the actual implementation begins by taking actions on the security risks. In this phase the selected controls will be applied to the target organization, the rest of the mandatory documentation will be finalized and the processes and procedures will be taken to use.

After the implementation of the security controls and the finalization of the documentation the ISMS will be reviewed by the ISMS organization.

The final step in the implementation phase is to internally audit the ISMS towards the ISO 27001:2013. This can be executed with the help of internal auditors for example from a different department of the company. If the organization has intentions to certify the ISMS, it will be possible with minimal effort after successfully executing previous steps of this thesis.

5.2.1 Execute risk treatment plan

Everyone from the target organization should be involved in the execution of the risk treatment plan and selection of security controls. Without the support of everyone it is not possible to implement the risk treatment successfully.

The actual execution can be kicked off by a workshop meeting. Risk owner stated in the risk treatment plan will have the responsibility to execute the risk treatment and monitor the risk treatment plan timeline and ensure that the planned actions are executed on time.

New risks and problems may arise along the process. These risks have to be documented and they should be addressed in the next risk assessment round.

5.2.2 Review ISMS

The next step is the review of the ISMS. This review is executed by the ISMS organization to see if something essential is missing, such as required documentation. In the review all the required documents are checked and published to the channel, most often a documentation system used to communicate the ISMS.

In practice the review can be done in a series of workshops where the ISO 27001 standard is analyzed and compared to the existing ISMS. Even though all areas should be covered, it is essential to verify that they are.

The purpose of the review is to verify that the risk treatment plan is effective, it is executed properly and there are no major inadequacies in the ISMS. All anomalies are documented to the SoA and are taken into the next risk assessment round to consider.

5.2.3 Internal audit

Internal audit is a phase where the ISMS will be audited for the first time. This audit shall be done by the persons inside the organization but in such a way that the objectivity of the audit will be guaranteed [1]. Persons doing the audit can be people outside of the specific organization that is in the scope of ISMS but still inside the company or upper organization.

The ISO 27001 standard requires that the organization will plan, establish, implement and maintain an audit program. The program have to consist of the continuous plan of the audits and the audits have to be performed at defined intervals throughout the year. The program should also include the methods, responsibilities and planning the requirements and reporting. [1]

The ISMS organization have to take the responsibility to create and execute the audit program. ISMS manager has the responsibility to monitor the execution of the program and ensure the objectivity of the auditors. Persons executing the audit cannot be the same that have reviewed the ISMS in the earlier step.

The standard also requires that the management should review the ISMS with defined intervals. Through these audits, the management is able to ensure the continuing suitability, adequacy and effectiveness of the ISMS [1]. ISMS manager has the responsibility to lead and monitor the audits and the audit program.

5.3 Continuous improvement

After ISMS has been successfully established and implemented the organization can proceed to the continuous improvement phase. As the ISMS is a long term process, the organization must develop their work constantly. ISO 27001 standard requires improvements meaning that not everything needs to be mitigated and compliant to the standard in the implementation phase but in the long run risks have to be addressed.

Not only the risks found in the first risk assessment session should be addressed but the risk assessment should be repeated in defined intervals to keep track on the vulnerabilities and risks concerning the organization. As the information security environment is constantly changing, eyes have to be open.

These three steps presented in this thesis as a continuous improvement phase are the steps to initiate the ISMS maintenance procedures. After the development plan is in place, the ISMS organization is responsible for following and executing it.

5.3.1 Establish a development plan

ISMS organization is responsible for establishing the development plan. Organization shall follow this plan and is committed to act on the risks and vulnerabilities found through this process.

To ensure that the ISMS is effective and it remains suitable and adequate organization have to assess and review the ISMS. Development plan should state the scope, criteria, frequency and methods how the organization will maintain the state of the ISMS [16]

As an input the development plan should take results of the internal and external audits and reviews, feedback from interested parties, follow-up actions from previous reviews and the recommendations for improvement [16].

As an output organization identifies the nonconformities and related corrective actions to improve the quality and effectiveness of the ISMS [16]. Example of a development plan template is illustrated in Figure 5.5.

Statement of Applicability chapter consists of a verbal description of the Statement of Applicability document. It will clarify the status of the ISMS in a short way. Scope of the development plan defines the boundaries of the plan. It states what

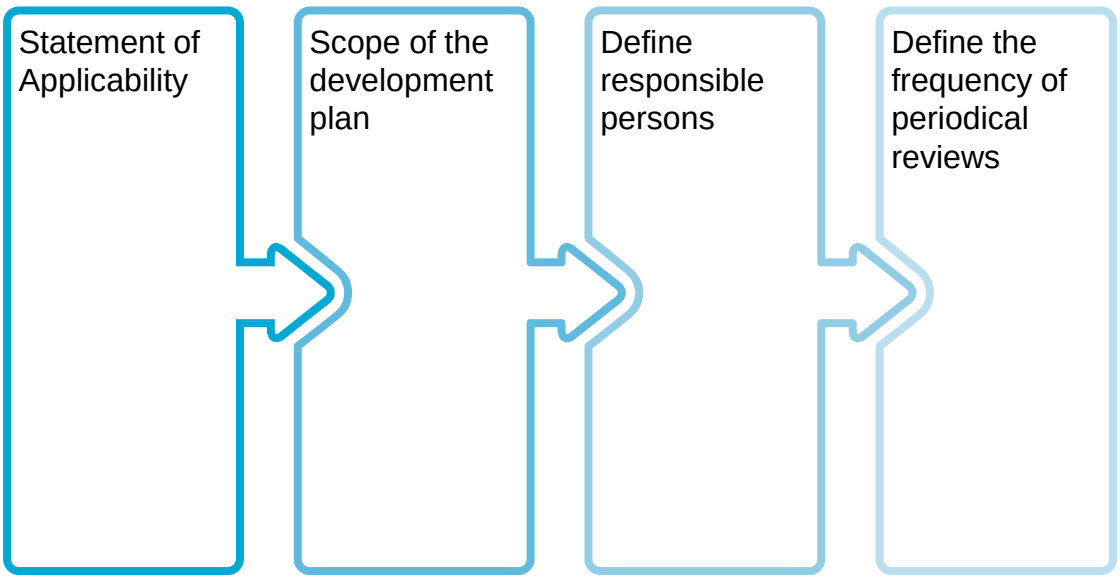

Figure 5.5 *Example ISMS development plan description*

areas are included or excluded from the plan. Responsible persons has a documented list of the updated ISMS organization list and will define the persons responsible of the designing, planning and implementation of the development plan. Finally a frequency for executing the maintenance phase has to be established.

5.3.2 Periodical audit of the ISMS

A Periodical audit has to be executed according to the development plan. The aim of the periodical audit is to update, assess and improve the state of ISMS.

In this review risk assessment is driven and the risks identified in the previous risk assessment are taken into account. If previous risks have not been mitigated as planned the mitigation plan should be escalated higher up in the management chain.

As the previous risks are verified to be mitigated new risks are supposed to be found. The environment, employees, technology and other factors are constantly changing.

After the new round of risk assessment a new round of internal audit shall be done.

ISMS needs monitoring and all nonconformities should be addressed.

5.3.3 Corrective actions

Based on the input from the periodical review, corrective actions are executed. Every time the risk assessment is driven, risk treatment plan created, corrective actions are documented and executed by the risk owners.

After the first time the corrective actions are executed and risks mitigated, the organization can start following the development plan of the ISMS. After these steps the ISMS can be considered as implemented.

5.3.4 Maintenance

After executing these three main steps of the continuous improvement phase the organization can shift to ISMS maintenance phase. The development plan will act as an input for the maintenance phase. Maintenance consists of three key steps which are presented in Figure 5.6.

Figure 5.6 *ISMS maintenance phase description*

The maintenance phase is in practice a cycle of actions. Risk assessment, risk treatment and internal audits have to be executed on a regular basis in order to keep the ISMS up-to-date and fully functional.

6. ESTABLISHING AN ISMS IN ERICSSON PSIRT

Establishing, implementing and improving ISMS is a long term process which requires management commitment as well as commitment from all team members. In the scope of this thesis only the establishment of the ISMS is done for PSIRT. This thesis will not cover further actions in Ericsson PSIRT.

Ericsson already has an ISMS in place at a global level but now the purpose is to establish the ISMS and start developing it in a team level. Team level ISMS will also ensure that the controls the global ISMS sets are in use and followed. As the global ISMS is on a high level the team level ISMS will offer the opportunity to take action on very specific things and therefore raise the information security level by addressing the risks that cannot be found during the risk assessments in the global level. As Ericsson PSIRT operates in Ericsson Network Security it is very important to follow best practices and guidelines in order to be able to deliver such values to customers.

6.1 Management commitment

As this thesis topic was raised by the management of Ericsson PSIRT, it was obvious that there will be extensive support for the work. As the implementation of ISMS is part of the PSIRT development plan, resources for the ISMS related work are allocated. Workshops for the ISMS were executed when PSIRT members did have a sufficient time available. This set limitations for the timeline and the amount of resources available at given times.

As stated earlier in Chapter 5.1, the most important aspect in the management commitment task is to establish ISMS organization to be responsible of the ISMS. ISMS organization was defined for Ericsson PSIRT as Figure 6.1 explains in general level.

ISMS organization consists of the PSIRT owner and two subgroups. The owner of PSIRT is ultimately responsible for information security. ISMS steering group is

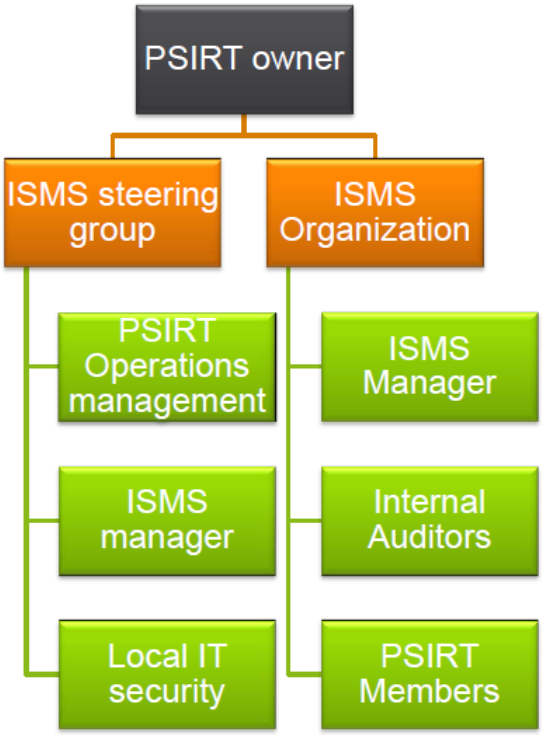

Figure 6.1 *Ericsson PSIRT ISMS organization chart*

basically the group that is supporting the ISMS and providing resources, funding and operational steering for the actual ISMS organization. ISMS organization consists of the ISMS manager, internal auditors and the actual PSIRT members chosen to be part of the ISMS activities. PSIRT members in the ISMS organizations are part of the development of ISMS. They also act as risk owners and therefore are responsible for the maintenance of the ISMS.

6.2 The scope definition

In a workshop held by the ISMS organization the scope for Ericsson PSIRT ISMS was defined. Defining the perfect scope is essential and can be hard especially when dealing with an organization that serves over 100 000 employees and different kinds of organizations all over the world.

In this case the scope definition became clear. PSIRT ISMS will cover all assets, services, PSIRT's internal IT infrastructure, employees and daily operations of PSIRT. The boundaries of the IT infrastructure are very strict. PSIRT ISMS only covers the communications networks, servers and equipment that are in the control of PSIRT. Nothing more is in the scope.

The scope definition was documented and is maintained by the ISMS organization

to the documentation system.

6.3 Risk assessment

As the ISO 27000 standard family is a risk based information security management framework, the most important and resource demanding part is to have a thorough risk assessment.

Risk assessment for Ericsson PSIRT was held in three different workshops. All the PSIRT members and two external drivers for the risk assessment were present. RA (Risk Assessment) drivers were external to ensure the objectivity of the risk assessment.

The first workshop was to identify all PSIRT assets. As some initial work had already been done around the topic the method for assessing risks was chosen to be the traditional asset based risk assessment. In the asset based risk assessment all assets are first identified. After the identification all assets were classified from the importance point of view. Also the owner of the asset was defined for each asset.

The second workshop was the main RA workshop. By going through the asset list all risks related to them were identified. Risks were found by discussing, brainstorming and making questions to each other. Here the objectivity of RA drivers is very important because internal team members tend to make things look better than they are.

In some cases risk assessment can be intimidating. For example when knowledge of a specific system or process has been concentrated to one person it can be recognized as a threat to the organization and the responsibility should be distributed. The person sitting on top of the knowledge can feel intimidated and be afraid of losing his advantage in the organization. That is why the risk assessment should be driven in general level and very gently but still deep enough so that all risks are addressed.

In Ericsson PSIRT such difficulties did not exist and the RA was driven very thoroughly. Even if PSIRT offers information security services and the level of security is high, some risks were identified during the workshop.

In the third workshop the risks identified in the previous step were evaluated. The evaluation of the risks is based on the Baseline Security Requirements used in Ericsson product development. Risks are evaluated based on the probability of the threat to materialize and the business impact i.e. the consequences of this materialization. Figure 6.2 presents the matrix used to rate the risks.

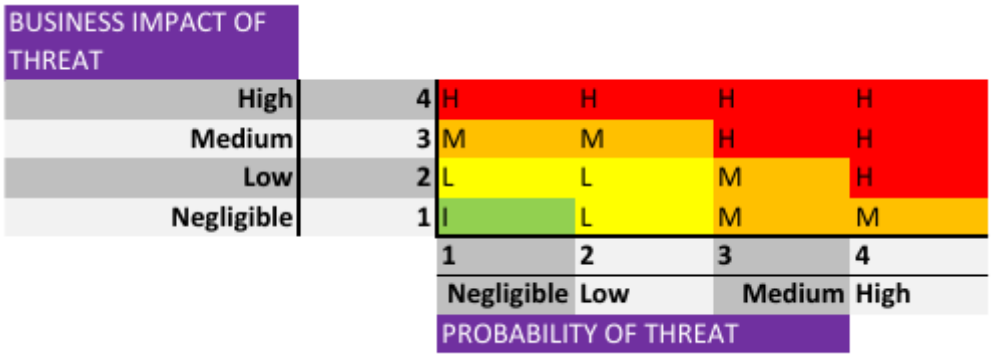

Figure 6.2 *Risk matrix used in the RA of Ericsson PSIRT*

6.4 Risk treatment plan

In order to have effective ISMS risks found in the risk assessment have to be mitigated properly. There are no recommendations which controls one has to implement to a certain kinds of organizations. As a first step it was decided to create a risk treatment plan without taking inputs from the standard.

A risk treatment plan for each risk found in the risk assessment was initiated in the risk treatment workshop. Each risk and possible mitigation was discussed and documented to the risk treatment plan. Risk owner was also decided for each risk from the ISMS organization. The risk owner is responsible for taking actions on the risk as defined in the treatment plan. Risk owner also monitors the progress in risk treatment and will report to ISMS manager if there are difficulties in the risk mitigation.

After identifying the best way to mitigate each risk, the planned actions were reflected to the ISO 27001 control list. Corresponding controls to represent the risk treatment plans were selected and documented to the risk treatment plan.

After specifying an owner and a risk treatment plan for each risk, the control list from the standard was analyzed as a whole. Some of the controls were selected as they acted as an input for new risks. These new risks found were documented to risk treatment plan but also to the risk assessment report as an additional note. This indicates that even though the risk assessment was done very carefully, some of them were still missed. For that reason it is very important that the ISMS organization is constantly working to identify new risks and will drive the risk assessment at specified intervals.

It was also found out that most of the controls from the standard were already in place but not documented and followed systematically. ISMS will improve this by

providing an organization and a system to execute the daily tasks in more secure manner.

Risk treatment plan and the selection of the controls was done in several separate workshops with Ericsson PSIRT members. A representative from PSIRT management was also present.

6.5 Statement of Applicability

After the risk treatment plan was established, a statement of applicability was created by Ericsson PSIRT members. An Excel tool was used to help creating a systematic list of the security controls in use. Several control objectives were excluded as they were not part of the scope of the ISMS.

A summary of the statement of applicability document was created among the actual document and the state of the ISMS was communicated onwards to the ISMS steering group.

7. ISMS FROM A CERT ORGANIZATION ASPECT

Information security is not something the organization can apply easily. It is a very long term process as presented earlier in this thesis. Computer emergency response teams are working in the center of the information security field by providing security services and consulting to other IT players.

It is common that these organizations may feel that they have a good control over their own organizational information security because there is a lot of information security knowledge in these teams. A CERT is constantly following the latest security threats, media, vulnerabilities so they are aware of the best practices and information security standards. That can create an unrealistic picture of the internal level of information security. CERT teams will easily advice other teams to have their business continuity plans and risk management procedures but have they ever considered what is the real status of themselves?

Information security management system (ISMS) is a great framework for establishing, maintaining and developing the information security in the target organization. ISMS is very suitable for a CERT if it is implemented with a common sense in mind. As seen from the implementation of the ISMS for Ericsson PSIRT, ISMS is a heavy duty package and cannot be implemented thoroughly immediately. The implementation of ISMS requires time and effort from the target organization as well as from external consultants or ISO 27000 competent people.

The most important thing from the common sense point of view in implementing ISMS for a CERT is to gain knowledge of the internal assets and risks related to them. When assessing all relevant assets from technical systems to personnel, a CERT is able to increase the level of information security drastically.

If there is no requirement of having the ISO 27001 certificate from customer or higher management it is no use obtaining it. However being compliant to the standard without a formal certification is very useful and can be recommended to all CERTs.

7.1 Advantages of the ISMS

The biggest advantage of the ISMS for a CERT is to point out the risks related to the operations, services and the ways of working. There are a great number of relevant documents produced as an output of the activities related to ISMS. These documents, such as risk assessment report or asset list can be also used as an evidence when justifying the funding for a CERT.

If a CERT has been working well for several years without any serious incident is it a result of a well working team or just lack of internal controls and monitoring systems? Without proper risk assessment and control over internal security of a CERT it is impossible to detect any malicious activity and damage caused to it. This is very basic information for CERT team members but the problem usually is that there is no time and funding for evaluating and developing the internal security.

Properly implemented, fully working and well maintained ISMS will guarantee the continuity of the information security risks for the CERT. It will point out the security issues that might be recognized but taken care of. There might also be blind spots in the risk surface of a CERT. ISMS will provide a systematic approach to manage information security risks.

7.2 Problems and limitations

The biggest problem with the ISO 27000 standard family is that it is a very general standard. If one needs to implement an ISMS and start the work based on the ISO 27000 standards, the implementation will require a lot of time.

After all there are numerous ways to implement the ISO 27001 requirements into the organization. There is a lot of space for misinterpretation in the control objectives and controls. It can also be difficult to even define the scope for the ISMS if the organization does not have experience over the ISO 27000 standard.

Another problem is if the target organization has a requirement to certify. That can lead to a point where the most important intention is to get certification, not to execute the required actions properly. It is possible to create documents required by the ISO 27001 without a correlation to the real world. For example risk treatment plan can be created but the actions for mitigation can be totally unreasonable and will not mitigate the risk. Also if the asset identification has not been done properly, the most important risks might still remain hidden.

ISMS will require a lot of time and effort from the target organization. It cannot

be bought as a service package outside the organization even though help from an external consultation company might be needed during the process.

7.3 Cost estimation

Based on the results gained during the implementation of ISMS for Ericsson PSIRT, a rough estimate of the implementation costs can be formed. With Ericsson PSIRT each phase, establishment, implementation and continuous improvement, took about 150 man hours. Overall hourly cost is therefore 450 man hours for the main phases. Additional hours from documentation, arranging workshops and research around the topic should be taken into account as well.

When the ISMS is implemented the maintenance of the ISMS will not require significant resources and funding. Annual risk assessment workshops and the documentation will require additional 150 man hours per year. Cost of having the ISMS is lower than the advantage gained from it. The advantage is hard to measure because the advantage is based on the risks that might realize.

7.4 Certification process

If a CERT needs to demonstrate the ISO 27001 compliance or such requirement is presented to a CERT in other way, the certification process will be initiated. The certification process is usually driven by an external certification body. This certification body will execute a gap analysis between the target organization ISMS and the ISO 27001 standard requirements. Gap analysis is an analysis which compares the requirements set by the ISO 27001 to the existing ISMS and as an output the organization will get information on what is missing and what should be implemented in order to be fully compliant to the standard. By choosing an accredited certification body the organization can ensure competence of the external auditor.

After the gap analysis a time will be given to fill the gaps found. After a period of time auditors from the external certification body will audit the ISMS. If the requirements of an ISMS are fulfilled the certification body will certify you as ISO 27001 compliant organization. The certificate will be valid three years from the initial certification. After that a new round of gap analysis and ISMS audit is needed to maintain the certification status. [24]

8. CONCLUSIONS

This thesis provides a guideline on how to implement ISMS (Information Security Management System) for a CERT in an effective way. The basis of the ISMS in this thesis is the ISO 27000 standard family which was developed by the International organization for standardization. This thesis presents one way to implement the requirements of ISO 27001 standard and as a result a CERT will have a fully ISO 27001 compliant information security management system.

CERT (Computer Emergency Response Team) is an organization that is responsible for the vulnerability coordination, incident response actions and other information security related tasks in their constituency. In practice this thesis was used as a starting point when implementing ISMS for Ericsson PSIRT team in Finland. Ericsson PSIRT is responsible for the product security in Ericsson worldwide.

ISO 27000 standard family consists mainly of three key standards, ISO 27001, ISO 27002 and ISO 27005. ISO 27001 sets the requirements for the ISMS. ISO 27002 has implementation guidance for each of the requirements which are called security objectives and controls in the ISO 27001 standard. Therefore the ISO 27002 is a code of practice and it helps in the implementation of the security controls. ISO 27005 includes the risk management process developed by the ISO. ISO 27005 is used in this thesis as a reference risk assessment method.

As the ISO 27000 standard family is written on a general level, it is not easy to just take the controls in use in the target organization. ISMS requires a lot of time and resources. This thesis offers a clear, effective and systematic way to understand and implement the ISO 27001 compliant information security management system in a context of a CERT. Implementation of the ISMS has been divided in the three main phases which are establishment, implementation and continuous improvement.

In order to have a fully operational ISMS, an ISMS organization has to be established. The ISMS organization will be formed from the team members of the CERT and it is responsible for the implementation and further maintenance of the ISMS. Certification process will be excluded from this thesis as it is not a common require-

ment for a CERT as of today. After executing the ISMS implementation according to this thesis the certification process can be initiated and driven with minimal effort.

The main advantage of the ISMS is to have a systematic view to CERT's information security risks. Risk management procedures are established if they did not exist. That means that the CERT will have to identify, assess and mitigate existing risks. Even though CERT is an information security team, it does not mean that the state of internal information security is adequate.

BIBLIOGRAPHY

[1] ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements, International Standardization Organization, 2013.

[2] ISO/IEC 27002:2013, Information technology - Security techniques - Code of practice for information security controls, International Standardization Organization, 2013.

[3] ISO/IEC 27003:2010, Information technology - Security techniques - Information security management system implementation guidance, International Standardization Organization, 2010.

[4] ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management, International Standardization Organization, second edition, 2011.

[5] ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management (second edition), 2014, IsecT Ltd., Available: http://www.iso27001security.com/html/27005.html

[6] Common Criteria for Information Technology Security Evaluation, Available: http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf

[7] Trusted Computer System Evaluation Criteria, Department of Defense Standard, 1985.

[8] Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonised Criteria, Office for Official Publications of the European Communities, 1991.

[9] COBIT 4.1, Executive Summary, Framework, IT Governance Institute, 2007, Available: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

[10] An Introductory Overview of ITIL 2011, itSMF UK The IT Service Management Forum, 2011, Available: http://www.best-management-practice.com/gempdf/itsmf_an_introductory_overview_of_itil_v3.pdf

[11] What is CSIRT?, European Union Agency for Network and Information Security (ENISA), 2005-1014, Available: https://www.enisa.europa.eu/activities/cert/support/guide2/introduction/what-is-csirt

[12] The ISO story, International Organization for Standarization, 2014, Available: http://www.iso.org/iso/home/about/the_iso_story.htm

[13] ISO 9000 - Quality management, International Organization for Standardization, 2014, Available: http://www.iso.org/iso/iso_9000.htm

[14] K. Beckers, Goal-Based Establishment of an Information Security Management System Compliant to ISO27001, The Ruhr Institute for Software Technology, University of Duisburg-Essen, Germany, 2014.

[15] ENISA - CERT Inventory, 2014, Available: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

[16] ISMS Implementation Guide, atsec information security corporationm, 2007, Available: http://www.atsec.cn/downloads/documents/ISMS-Implementation-Guide-and-Examples.pdf

[17] Activity 7 - Guide to setting up a CERT, Available: http://www.terena.org/activities/tf-csirt/archive/acert7.html

[18] Friendship among equals - Recollections from ISO's first fifty years, 1997, Available: http://www.iso.org/iso/2012_friendship_among_equals.pdf

[19] Use offence to inform defense. Find flaws before the bad guys do, SANS Institute, 2003, Available: https://cyber-defense.sans.org/resources/papers/gsec/implementation-methodology-information-security-\T1\lmanagement-system-to-comply-bs-7799-requi-104600

[20] ISO 27001:2013 Mandatory Documents and Records, IBMS Consulting, 2014, Available: http://www.ibmsconsulting.com/documentation-required-iso-270012013/

[21] J. E. Siig, How to develop a Statement of Applicability according to ISO 27001:2013, 2013, Available: http://www.neupart.com/media/142730/how_to_develop_a_statement_of_applicability_according_to_iso_27001-2013-eng.pdf

[22] Information Security Management Systems Auditor/LEad Auditor Training Course (BS ISO/IEC 27001:2005) Course Notes, The British Standards Institution, 2007.

[23] D. Stiikvort, SIM3: Security Incident Management Maturity Model, S-CURE by PRESECURE GmbH, 2015, Available: `https://www.trusted-introducer.org/SIM3-Reference-Model.pdf`

[24] Certification to ISO/IEC 27001 Information Security Management, bsi., 2015, Availabe: `http://www.bsigroup.com/en-GB/iso-27001-information-security/Certification-for-ISO-27001/`