LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Implementing Finnish National Security Audit Criteria KATAKRI to Arctech Helsinki Shipyards Inc.

Mattsson, Jarkko

Laurea University of Applied Sciences

Implementing Finnish National Security Audit Criteria KATAKRI to Arctech Helsinki Shipyards Inc.

Degree Programme in
Security management
Bachelor's Thesis
May, 2018

Laurea University of Applied Sciences Security management
Degree Programme in Security management

Abstract

Jarkko Mattsson

Implementing Finnish National Security Audit Criteria KATAKRI to Arctech Helsinki Shipyards Inc.

Year 2018 Pages 40

The aim of this thesis was to describe a case project whose purpose was the implementation of Finnish national security audit criteria (KATAKRI) to Arctech Helsinki Shipyards Inc. Through the described project Arctech aimed to improve competitiveness in the ship building sector, increase overall protection of information within the company and bring the security into part of daily operations.

The thesis was conducted as a case study and it used qualitative methods such as data analysis/literature reviews, interviews and workshops to collect and share information regarding the project at the same time collecting background information necessary for the thesis.

The theoretical background is collection of information regarding KATAKRI and topics that are affiliated with set criteria. This theoretical section tries to open the KATAKRI itself in ways in which it works and what is the background information needed to understand KATAKRI better.

The methods section describes the methods used during the case project and information gathered from set methods leading to how the case project was conducted. This section also includes the case project in step-by-step form.

At the very end of this thesis are the results and conclusions. The results part is divided into two sections: general findings and an alternative simplified version on how Katakri work can be conducted. The conclusion part consists of key findings and development ideas for the future.

Keywords: KATAKRI, Information Security, Risk management, Case-project

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusala (AMK)

Jarkko Mattsson

Suomen kansallisenturvallisuusauditointikriteeristön KATAKRIN implementointi Arctech Helsinki Shipyard Oy:lle

Vuosi 2018 Sivuja 40

Lopputyön tarkoituksena on kuvata tapaustutkimusta, jonka tavoitteena oli Suomen kansallisenturvallisuusauditointikriteeristön (KATAKRI) käyttöönotto Arctech Helsinki Shipyards Oy:ssä. Tämän projektin kautta Arctech pyrki: parantamaan kilpailukykyä laivanrakennus sektorilla, nostamaan informaatioturvallisuutta kokonaisuutena yrityksessä, sekä nostamaan turvallisuuden osaksi päivittäistä toimintaa

Lopputyö on tehty tapaustutkimuksena käyttäen laadullisia metodeja kuten esimerkiksi data analyysillä/kirjallisuuskatselmoinnilla, haastatteluita ja työryhmiä. Näillä metodeilla pyrittiin keräämään sekä jakamaan tietoa liittyen projektiin, mutta myös samaan aikaan keräämään tarvittavaa taustatietoa lopputyölle.

Teoreettinen tausta lopputyölle muodostui kokoelmasta virallisista dokumentteja koskien KATAKRI:a sekä dokumenteista, jotka viittaavat KATAKRI:n. Teoreettisella osalla pyritään avaamaan lukijalle mikä KATAKRI on, kuinka se toimii sekä mihin kaikkeen se perustuu. Tämän avulla lukijan on helpompi ymmärtää tapaustutkimuksen aihetta sekä tuloksia.

Tämän lopputyön metodi osuus kuvailee tapaustutkimuksessa käytettyjä metodeja ja niistä saatua tietoa johtaen kuinka tapaustutkimus toteutettiin. Projektin toteutus on avattu kohta kohdalta.

Viimeisenä osana tätä lopputyötä löytyvät tulokset ja yhteenveto. Tulokset osuus on jaettu kahteen osaan: yleisiin löydöksiin sekä vaihtoehtoiseen yksinkertaistettuun version kuinka KATAKRI projekti voidaan toteuttaa. Yhteenveto osuus koostuu avain löydöksistä sekä kehitys ideoita tulevaisuutta varten.

Avainsanat: KATAKRI, informaatioturvallisuus, riskienhallinta, Casa-projekti

Table of Contents

1 Introduction 6
1.1 Project time usage 7
2 Case Arctech 7
2.1 Arctech Helsinki Shipyards Inc 8
3 Theoretical background 9
3.1 Audit 9
3.2 Risk management 10
3.3 ISO/IEC 27000 series and ISMS 12
3.4 KATAKRI 13
3.5 VAHTI 14
3.6 Security clearances 14
3.6.1 Facility Security Clearance 15
3.7 The general data protection regulation of EU 15
3.8 Protection of classified material 16
3.8.1 National 16
3.8.2 International 16
4 Methods 18
4.1 Data analysis 20
4.2 Workshops 21
4.3 Interview 21
4.4 Case project 21
5 Results 25
5.1 Recommendations based on the case project 28
5.2 Objectives of the thesis 31
6 Conclusion 32
6.1 For future development 33
6.2 Validity 33
References 34
Figures 37
Appendix 1 List of abbreviations 38
Appendix 2 Acting authorities of KATAKRI 39

1 Introduction

The purpose of this thesis is to explain the process of Finnish national security audit criteria (later KATAKRI) in simple terms and at the same time develop the KATAKRI preparation process so that it is easy to apply by companies. The thesis aims to guide companies on how the KATAKRI process works, how it can be used to develop information security within the company and why it is beneficial for a company to apply such information security.

KATAKRI is a Finnish national security audit criteria tool that gives guideline requirements on authorities and companies on how to achieve Finnish national security levels. The KATAKRI tool covers information security as a package that consists of three subdivisions: Security Management (T), Physical Security (F) and Information Assurance (I).

This thesis refers to a case project that was done in close co-operation with Arctech Helsinki Shipyards Inc. (Later Arctech). The need for the case project came directly from Arctech. The goal of the case project was to develop Arctech's information security management to follow KATAKRI criteria, thus leading to a more secure work environment. The case is described in sections 2 and 4.4. The results for case the project is described in section 5 and development ideas in section 5.1.

This thesis is divided in six (6) sections: introduction, case, theoretical background, methods, results and conclusion. The introduction states the goals and the purpose of the thesis. The case section describes the case project and the company that the project was made with. This opens what was the starting point and what was the desired result. Theoretical background covers theory regarding KATAKRI. The purpose of this section is to describe the theory for the reader showing why, what and who are the factors affecting KATAKRI. The methodology sections describe the methods that were used during the study. In this section the case project is described in detail. The results section describes the findings that were made during the case project and the suggestions for new development ideas to the KATAKRI process. The conclusion section sums up the findings from the case project.

Objectives for thesis were:
- Describe the KATAKRI process from the company viewpoint
- Help readers who might not be familiar with KATAKRI to understand what it is
- Develop a framework for KATAKRI implementation

1.1 Project time usage

The case project took place between 19.10.2016 and 15.6.2017. After that the thesis creation continued until January 2018. During the case project period work focused on updating and creating documents for Arctech Helsinki Shipyards Inc. (Later Arctech) for preparation on KATAKRI auditing. This also included interval reviews by an outside consultant who checked and approved created documents. Project work consisted of twelve parts that are illustrated in detail in section 4.4.

2 Case Arctech

The case project itself aimed to develop information security for Arctech, which would fulfil the requirements set by the Finnish national audit criteria KATAKRI. This was tried to achieve by creating documents that stated the company's policies and instructions on how to handle security and information security. The consultant then checked the created documents; this was done to verify that the documents are in line with the KATAKRI. If documents fulfilled all the necessary requirements, they were then implemented within Arctech's information management system (IMS) and if not, the documents were revised until they fulfilled the necessary requirements. The intention was that upon completion, this collection of management material could be used by Arctech to apply KATAKRI certification from Finnish National Security Authority (NSA), meaning that Arctech would have the approved level of information security set by Finland.

The requirement for the KATAKRI standard came directly from Arctech; their senior management had decided that it would be beneficial for Arctech to acquire this level of certification. This would develop shipyards' general security (Physical and information) and open up possibilities for new businesses, such as designing and building ships for Finnish Defence Forces or participating in international projects, which require security clearances. The benefits of this case project were the development of information security processes and improving business continuity/sustainability.

At the beginning of this thesis project, Arctech's overall state of security and information security documentation was reviewed. In general, the state of Arctech's existing security documentation was adequate compared to KATAKRI criteria, but the review showed that the state of information security documentation was completely out of date, and therefore updating this documentation came to be the main focus of updating documents.

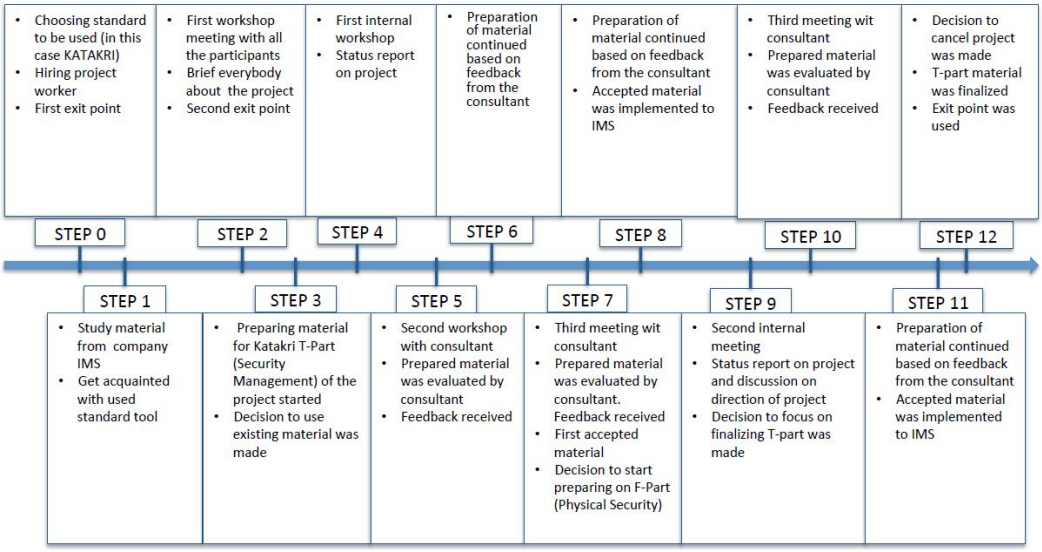

Figure 1 Overview of the case-project

Figure 1 above shows the overview on how the work was divided during the running of the case project. This gives a general idea in which order the actions were completed and what steps were achieved during the case project. This figure is referred to later from page 22 onwards (STEPS of the case project) where a thorough breakdown of the case project is located.

The next step in the case project would have been the preliminary audit to determine if there was a need for alternate material or the secured facilities. The Preliminary audit phase was not conducted during the thesis, but the plan was that the project would continue at a later date.

2.1 Arctech Helsinki Shipyards Inc.

Arctech Helsinki Shipyards Inc. is owned by the Russian United Shipbuilding Corporation (USC). The company was established in December 2010 and Arctech started its operations on 1st April 2011. Arctech employs approximately 1400 persons of which around 600 (360 construction workers and 263 management employees) are Arctech's own employees and the rest work as subcontractors. The company is located in the Helsinki district of Hietalahti, Finland. (Arctech, 2017)

Arctech has a long history and experience in building arctic vessels. Helsinki Shipyards was established in 1865 and since then more than 500 ships have been built at the facility. The shipyard has developed the majority of the icebreakers, offshore vessels and arctic tankers in

operation around the world. Arctech has a long history, and they are not only experienced but also the forerunner in developing and applying technological innovations. (Arctech, 2017)

3 Theoretical background

Literature helps to understand studied phenomena and offers tools for the writer in different phases of the work process. The literature used can be divided into two categories: Literature that is related to the topic and literature regarding methods of research. (Kehittämistyö opinnäytetyönä, p.88)

Literature is needed to back up the theoretical framework. Resources consist of theories, models, previous research and reports that explain the phenomena. In the thesis the writer become familiar with previous studies written in the field or topics regarding the writer's own research problem. Materials cannot cover the research problem at a general level but must be relevant to the research problem studied. There must be strong ties between writer's own work and the literature chosen. (Kehittämistyö opinnäytetyönä, p.88)

The case project used the Finnish national security audit tool (KATAKRI). To understand it is crucial in understanding information security in general. There are multiple ways to conduct information security and there are many factors that affect it. The theoretical section tries to collect central topics regarding KATAKRI and information security in one package. This should give the reader an understanding of what are the basics of KATAKRI, where it is based, how it works and what must be taken into account when using it.

3.1 Audit

Auditing is an assessment of quality systems carried out by a neutral observer. According to Heikkilä, auditing can be divided on two different categories: Internal that is done by the company itself and External that is conducted by an affiliated company or third party. (Heikkilä, 2004) Anna Kohnke et al. (2016) describe the same division in respect of internal and external audits. They also state that in order for auditing to succeed the senior management has to agree on outcomes and actions that come from the audit.

Heikkilä (2004) states that "Most important aspect of audit is observing practical actions in company environment, this is done by assessing how well company's documentation and functions matches on affecting standards and is they sufficient". This means that existing documents and actions that the company produce on a daily basis are compared with each other. The auditing party creates a report on how well standards are followed and are there any deviations. This report is then passed on to company management who are responsible for

overseeing that necessary actions are taken to fix any deviations and further develop audited operations. According to Kohnke A, et al. (2016) the purpose of the audit is to gather sufficient, reliable, pertinent and practical evidence to demonstrate that defined security and performance control objectives are met.

During the case project auditing was planned to be held twice. The first time internally, when the necessary material and facilities were made ready, and the second time externally when the Finnish authorities were going to evaluate if Arctech is eligible to receive KATAKRI certification. The benefit of this type of approach would have allowed company to fix deviations before the external audit, which would have led to an organized external audit, due to the fact that all necessary materials/operations would have been collected and checked before they are handed over to Finnish authorities.

The auditing phases were not completed during the case project, because the project was cancelled before that phase was reached. Auditing was still an important part of the whole case project, and therefore it is vital to understand the basic principles because this affects the "tone" of the documents, meaning that the documentation must be precise.

3.2 Risk management

VAHTI describes risk management as follows "Risk management is a part of management and operational processes. It is also a part of planning and following. The aim is to have organizational decision making which is up to date, right and comprehensive enough to understand risk, but also clearly defines responsibilities and systems." (VAHTI 1/2017, 2016)

Tony Merna et al (2008) describe the purpose of risk management to identify organisation specific risks and respond to them accordingly. Merna, T, et al. also agree that every sector of an organisation should be included in the risk management.

One way to verify an organisation's level of security is to use different standards and standard tools that are risk based; for example, the ISO 27000 series and KATAKRI. This gives the organization an excellent tool to evaluate what types of risks are affecting the organization's own information and how to mitigate that risk. Also, through applying these standards organizations can show that they have reached a specified level of risk management. During the case project risk management was focused on security operations because this was the sector where the effects of the KATAKRI requirements would be felt the most and therefore there was a need to assess the current situation. By conducting a risk assessment on the security operations most of the parts in regard to physical and information security that needed improvement were discovered.

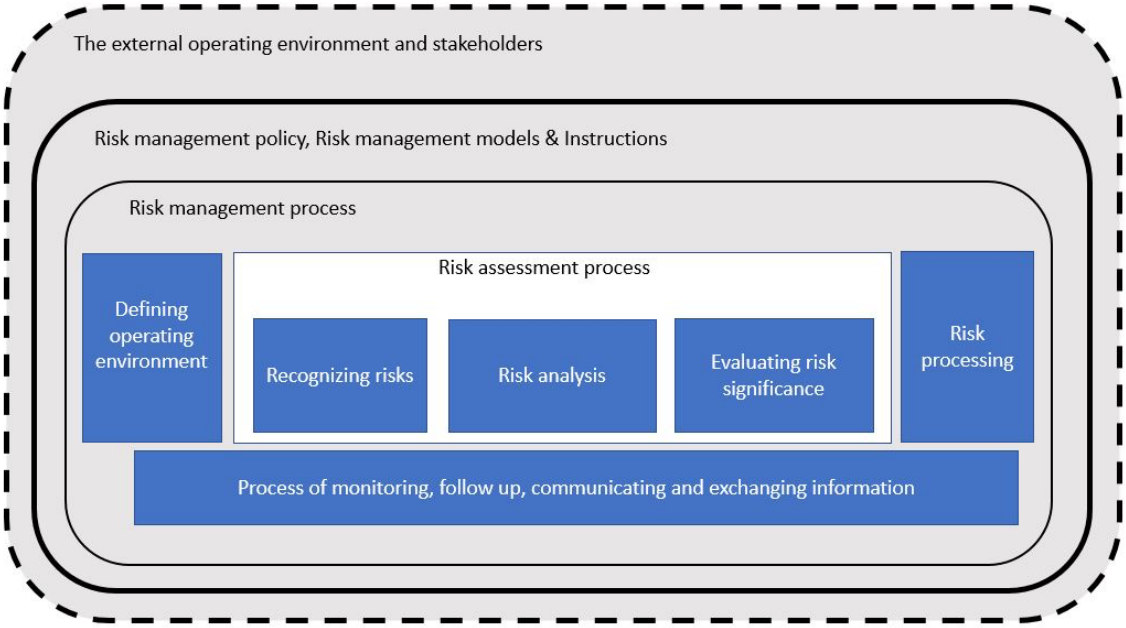

Figure 2 Risk management process (Vahti 1/2017)

Figure 2 illustrates the whole process of risk management. It must be noted that risk management aims for continuous improvement; therefore, it will not end after the risks are defined. The first level is defining the external factors e.g. the operating environment, what competition the company has and who the company is working with. The second level is how the evaluated measures are stated inside the company e.g. how well the employees are instructed and what the company policy states. The third level is the actual risk management process, first defining what is the evaluated part of the company. After that comes the risk assessment part during which the risks are recognised, analysed and evaluated. This gives information on what the actual risks are, leading to decisions on how the identified risks should be handled. End results can vary, from improving instructions to changing operating methods. The last step is the monitoring, through which the company can follow changes in risk levels. Following might also enable the company to discover new risks that were not identified during the risk assessment and take them into account.

Risk management is a crucial part of organisation management because it gives crucial information for the company, helping the organisation to separate risks that must be removed and what level of risks the company is willing to accept. For this same reason risk management and risk assessment are also important parts of the standardisation, which has this standardised level of risks that an organisation should not exceed. By fulfilling standardised requirements the company can show that it is not taking unnecessary risks.

3.3 ISO/IEC 27000 series and ISMS

According to Georg Disterer (2013) “there is urgent need for information security measures, due to that fact that information and information systems are an important foundation for the companies”. This need is due to information sharing that companies conduct over open networks, which exposes the information and the information systems to external hazards. For this reason companies need adequate control over their information security. This can be achieved by using the widely known and accepted ISO 27000 series of standards. (Disterer, 2013)

ISO standards are provided in a “series”, meaning that all standards relating to specific field are collected under one “series”, which are marked with numbers. The ISO 27000 series was developed to be the standard for information security and originates from British Standard BS 7799. To ensure that an organization has fulfilled the necessary requirements it usually undergoes an audit conducted by an accredited auditor.

ISO/IEC 27000 series consist of:

A) Define requirements for an ISMS and for those who certify such systems
B) Provide direct support, guidance and/or interpretation for the overall process to establish, implement, maintain and improve the ISMS
C) Address sector-specific guidance for the ISMS
D) Address conformity assessment for the ISMS
E) State key terms and definitions

ISMS is a systematic approach to an organization’s information security to achieve its business objectives. To ensure an organization’s data protection an ISMS consists of different types of measures. These measures are policies, procedures, guidelines, associated resources and activities, which creates a system that covers data protection on multiple levels. To minimize risks on information security and effectively treat / manage risks the ISMS is based on risk assessment and an organization’s risk acceptance levels. This allows the organization to decide at which level they are willing to operate. (ISO/IEC 27000:2017)

As previously mentioned, ISMS is based on risk acceptance. This means the level of risk that the organization is willing to take or accept to gain value. In broader terms this means that the organization gives up something in exchange for gaining something else, but by also accepting the risks that the decision brings with it. For example, company A decides that production of rubber boats should be moved from Finland to China. This would mean that probably production costs would go down, but there is a risk that deliveries are delayed due to long

distance. The organization accepts this risk because the benefits exceed the risk. This same principle can be applied to the protection of information.

During the case study the ISO 27000 series was studied because KATAKRI refers directly to this standard. This is because the requirements stated by KATAKRI are developed from standards stated in the ISO 27000 series, the only difference being that they are taking into account the viewpoint of the Finnish national authority.

3.4 KATAKRI

Finnish national security auditing criteria (KATAKRI) is a standard and auditing tool whose purpose is to measure the information security of a company at all levels of security, from company policies to individual work instructions. To show that a company has achieved the necessary requirements, a certificate is issued after an audit with Finnish authorities. Arctech chose the KATAKRI standard to be used in the case project, because they saw that having this would benefit the company in the future. With this standard Arctech could show customers that data protection in this company is at a good level. Some customers require this standard to be in place before they even begin contract negotiations.

The KATAKRI standard was created as part of a Finnish Governmental program for internal security. The standard was prepared in cooperation between the Finnish authorities, Finnish industries and specialists in the security field. As a standard, KATAKRI has two significant traits, that differs from normal standards. Firstly it makes the actions of responsible authorities work transparent and equal towards everybody. Secondly, it allows Finnish industries to be more cost effective by making the authorities' requirements foreseeable. (KATAKRI II, 2011) Since the initial publication of KATAKRI it has been completely updated twice, in 2011 and 2015. The Ministry of the Interior is responsible for further managing and updating KATAKRI. (KATAKRI, 2015)

Even though KATAKRI is a standard tool it does not set mandatory requirements on information security, but rather states minimum requirements, which are based on national legislation and international security obligations. Most important of these are – at the national level the Government Decree on Information Security in Central Government (681/2010) which sets the foundation of both national and international Classified Information - and at the international level the Council Decision on the Security Rules for protecting EU Classified Information (2013/488/EU), which lays down principles and minimum standards of security for protecting EU Classified Information (EUCI). (KATAKRI, 2015)

3.5 VAHTI

The Governmental Information and Cyber Security Management Board (VAHTI) appointed by the Ministry of Finance is responsible for steering, developing and co-ordinating efforts in the area of information security in central government. (Ministry of Finance, 2017) VAHTI processes all significant policies on information and cyber security as well as matters related to steering of activities in the field of information security in central government. In the measuring of information security, VAHTI is an international forerunner. Its annual information security survey is used as the basis for creating of annual description of the state of information security in Finnish central government, the summary of which is published each year in the VAHTI annual report. (Secure Finland, p.116, 2015) The general obligation for governmental authorities to be aware of information security is based on Act on the Openness of Government Activities (621/1999). (Turvallinen Suomi, p.121, 2015, translated by thesis author)

During the last update of KATAKRI in 2015 the Ministry of the Interior decided that KATAKRI should be updated less often. This decision came about probably because they realized that keeping this type of document up to date is almost impossible. Therefore, by using VAHTI board published guidelines on data protection it can be guaranteed that KATAKRI stays up to date always.

3.6 Security clearances

Security clearances are divided into two categories; normal security clearances (covered in 3.6) or Facility security clearances (covered in 3.6.1). Security clearance generally refers to checking a person's background for a certain purpose and Facility Security Clearance (FSC) refers to checking company backgrounds. In regard to this case project background checks would have been conducted on implementation of KATAKRI requirements and during the creation of documents these factors had to be taken into account.

The Finnish police stated the Following on security clearance: They refer to checking the background of persons who participate in crucial parts of society or need access to sensitive material. (Police of Finland, 2017) The reason for conducting background checks is to prevent any action or crime that may pose a threat to the internal security of the country, the national economy, or major companies that are operating in the nation. The reason might also stem from an international obligation. Types of personal background checks are: concise, standard and comprehensive.

The Finnish Security Intelligence Service (FSIS) is responsible for conducting standard and comprehensive security clearances. These are conducted to determine whether a person may, for work purposes, be granted access to specific information. Standard security clearances are conducted for companies and public authorities, whereas comprehensive clearances are conducted for public authorities only. Defence Command Finland (DCF) is responsible for all security clearances which fall under the jurisdiction of the defence administration. (Police of Finland, 2017)

3.6.1 Facility Security Clearance

When participating in international projects or tendering processes Finnish companies may handle international security classified administrative material. In these cases, it might be necessary to have a certificate that companies can handle this security-classified material properly. Certificates for international security classified projects also known as Facility Security Clearance (FSC) can be granted to companies through the National Security Authority (NSA) that is located in Ministry for Foreign Affairs of Finland in that case if the company has a valid security agreement with the Finnish Security Intelligence Service (FSIS). (FSIS, 2017)

3.7 The general data protection regulation of EU

General data protection regulation (GDPR) is the newest addition to data protection. GDPR is the core element of the EU council's data protection reform. This regulation aims to update and modernize principles of the old data protection directive that was set in 1995. GDPR aims to set out and clarify rights of the individual and establish obligations / responsibilities for those who oversee the processing of the data. This regulation also establishes methods for ensuring compliance as well as sanctions for breaching the rules. (EU council 2016) In addition to previous the GDPR aims to improve internal markets of EU by providing unified regulation.

The GDPR aims to:

- Give more rights and control to individuals over their own information.
- Give clear obligations to the person controlling or handling the data.
- Create consistency across the EU regarding data protection.
- Remove unnecessary bureaucracy. The principle of the one stop shop aims that the person/company has to deal with only one country's data protection authority.

Figure 3 Content of general data protection regulation

During the case project GDPR was one of those topics that had to be considered when planning the documentation for the KATAKRI project. This was because even though this directive was not in force during the case project it will set requirements in the future in relation to Finnish legislation and therefore affect KATAKRI requirements. This affects document creation so that they should also cover the requirements set by the GDPR. Otherwise the documents have to be re-written when the GDPR comes in force.

3.8 Protection of classified material

This section covers what legislation affects the protection of national and international materials. The international section covers in general how to handle international material, but also EU and NATO materials. It is necessary to understand this legislation, because they directly affect the company.

3.8.1 National

In Finland the protection of secret documents is based on the Act on the Openness of Government Activities (JulkL 621/1999) that states the scope of application following: ”This act contains provisions on the right of access to official documents in the public domain, officials duty of non-disclosure, document secrecy and any other restrictions of access that are necessary for the protection of public and private interests, as well as on the duties of the authorities for the achievement of the objectives of this Act”(Ministry of Justice, 2016).

The Finnish national audit criteria (KATAKRI) is based on this same Act (JulkL 621/1999). Information security agreements provide the framework for the participation of Finland and Finnish companies in projects that require the exchange of classified information. (Ministry of Foreign Affairs of Finland, 2017) These agreements are known as GSA’s (General Security Agreement). On these agreements the requirements are set and mutually accepted between Finland and the country that the agreement concerns.

3.8.2 International

International classified material means specially protected information resources that are mentioned in law (588/2004) regarding information security obligations, which Finland must

protect according international agreements or European Union security provisions. (NSA, 2016) This legislation affects both authorities and Finnish industries when they are participating in projects that need security clearance. Governmental authorities are responsible for ensuring that Finnish industries are capable of handling internationally classified information. General international regulations are taken into consideration in Finnish national security audit criteria (KATAKRI), which is used as a tool by the Finnish authorities when they are confirming the security clearance of Finnish industries. (NSA, 2011)
To ensure that security classified material is protected accordingly, EU and NATO enforces this by setting up mutual agreements between Finland and the agreeing party. These mutual agreements are as follow:

To ensure protection of EU classified information in European member states, the EU commission has made a decision (2013/488/EU) to set security rules that define the basic principles and minimum standards concerning EU classified information. In this act, the security levels of information are defined in four levels (shown in figure 4). Finland enforces this by legislation (588/2004).

To ensure the protection of NATO documents mutual information security agreement between NATO and Finland has been made (SopS 7 and 8/2013). In this agreement both parties agree to protect security-classified material. NATO has a separate internally accepted code for handling security-classified material. In this agreement, Finland has committed to respect requirements with necessary national measures that are stated in NATO code." (NSA, 2016)

Protection of NATO classified materials is connected to KATAKRI because there are multiple nations within EU that are part of NATO. Finnish national measures are in line with NATO code, which means that requirements set by KATAKRI are also sufficient to protect NATO documents due to that fact that they are based on the Act of openness of Government Activities (JulkL 621/1999).

Security Classifications		
European Union Security class	**Finnish Security Class**	**NATO Security Class**
TRÈS SECRET UE/EU TOP SECRET	Erittäin salainen/Ytterst hemlig	Cosmic Top Secret
SECRET UE/EU SECRET	Salainen/Hemlig	NATO Secret
CONFIDENTIEL UE/EU CONFIDENTIAL	Luottamuksellinen/ Konfidentiell	NATO Confidential
RESTREINT UN/EU RESTRICTED	Käyttö rajoitettu/ Begränsad tillgång	NATO Restricted

Figure 4 Security clearance levels

Figure 4 depicts how security classification levels are in comparison to each other. Unifying the security levels prevents misunderstanding and incorrect labelling of classified materials.

4 Methods

This chapter describes the methodology that was used during the case project. A case study was chosen as the research strategy, and research was done using qualitative methods. The case study was the best choice due to the fact that the project consisted mostly of analysing data from different sources, the research topic came directly from a company and it focuses on a specific part of the organization.

In general terms case study means studying some specific case or phenomena. Case studies research one or multiple cases or phenomena. As a term, “case study” is widely used in psychology and business administration. For example, the research of Freud and Jung are based on case studies and theories that are drawn from them. These are examples of qualitative research. (Kehittämistyö opinnäytetyönä, p.34)

According to Peter Swanborn (2010) the case study can be divided in two categories: extensive and intensive, where extensive data is gathered from multiple sources in regard to the studied phenomena, and intensive focuses purely on one specific case and its phenomena. (Swanborn, P 2010) By using the intensive approach to the phenomena allowed studying of this specific instance and therefore gave specific results in regards to how well this tool works on studying the specific target company. For this reason, the case study was chosen to be the main research strategy in this thesis. Also, because typically research materials for case study consist of different type of documents, archives, interviews, observations, etc. it suited per-

fectly this specific project. These types of materials formed the theoretical background for this thesis.

Kaunanen, J describes the study target as follows: The studied unit or case can be a company, community, part of an organisation, a group of people or an individual, which are observed in the real-world environment (context). The case study is not really a study, but rather an approach method, which can have characteristics from qualitative and quantitative case study. (Kehittämistyö opinnäytetyönä, p.34-35) This research of real world phenomena also affected the decision to use case study for this specific thesis.

Qualitative methods were chosen because they gave specific and solid answers to problems that phased research during the case project. “Qualitative research is describing ‘real life situations’. In qualitative research the subject of research is studied comprehensively. The results are limited to conventional explanations limited to a certain time and place. In general, the aim of qualitative research is to find or reveal facts rather than verifying existing claims.” (Tutki ja kirjoita, 2013) During the thesis three different types of qualitative methods were used to obtain information and find solutions. These methods were data analysis, interview and workshops. These methods were chosen because they were most suitable for the case project that was done in cooperation with a company. These methods allowed collection of information, and at the same time, the sharing of information with Arctech regarding the project, creating a situation where data was collected through dialogue.

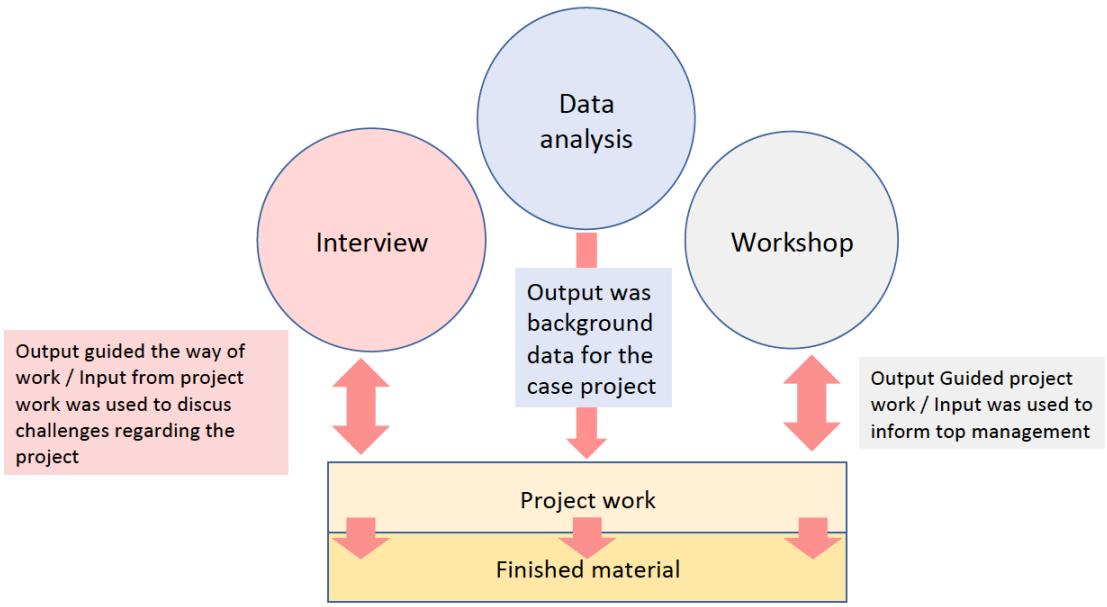

Figure 5 The case project workflow process

During the case project, literature and data analysis were used as a method to broaden the writer's understanding regarding KATAKRI. By using these methods, the writer was able to find topics, theories and methods that supported the case project. Literature analysis was used to find information on the studied topic (substance literature) and data analysis was used to study Arctech's information management system, which was used to determine the starting situation. By comparing existing documents to findings from literature analysis it was possible to create documents that fulfilled requirements set by KATAKRI. All the used methods are open in below as follows: the used method is described, what was the purpose, what was searched and lastly what were the findings.

4.1 Data analysis

In this thesis data analysis is referred as a method of analysing the organisation's documents and other documents which are related to the case study in order to determine the status of the organisation's documentation and to seek out related information for the case project.

To support findings from data analysis, systematic literature review was used. Jesson (2011) describes the purpose of literature review as a form to understanding of the current state and the environment of information. Within literature review targets are pre-defined and way how to approach the targets are decided beforehand. Systematic literature review means reviewing material that is chosen based on beforehand decided criteria. (Jesson, et al. 2011)

Reasoning behind choosing this method to support data analysis was the clear need to focus of company documentation and their relation to KATAKRI. Jesson (2011), also states that by studying the backgrounds properly it is possible to view current situation and possible deficient with in it. (Jesson, et al. 2011) Because of using limited and well-defined material with clear research goal the data analysis made during this project resembles systematic literature review thus its methods were used when the material was analysed for this project.

Data analysis was the main method for seeking information regarding the case project's topic (KATAKRI). The information search was conducted so that firstly all of the documents in Arctech's IMS were read through and evaluated. This gave a solid understanding of the status of the existing documents (what documents could be used as they are and what needed to be re-written). Secondly data analysis was used to seek information from outside sources. With this the requirements in regard to KATAKRI were looked at and at the same time the general knowledge background was expanded in order to understand the topic better. This part had a wide range of information sources including: documents from Finnish government, Finnish authorities / Finnish industries and academic writing from the field of information security.

From the findings the case project foundation could be gathered. This included: the state of the Arctech's documentation, requirements stated by the KATAKRI tool, what factors (legislation, regulations, standards, e.g.) must be considered when preparing the material and in general how to create documents so that they are in line with KATAKRI.

4.2 Workshops

In this thesis the workshop means the group of people which gathered on a regular basis to determine action and share information in regard to the case project (This is described in more detail in section 4.4). During these workshops the main focus was on sharing information and obtaining feedback from senior management. This was because it was necessary to create "logical" documents for the case project. This means that the created documents had to be in line with policies set by the Arctech therefore input from senior management was needed.

Workshops were organised so that two weeks before the workshop meeting invites were sent. This was done in order to define a date and place when and where everyone from the workshop group could participate. This also allowed re-scheduling of the workshop if needed. The workshop had two consistencies: internal and external. The internal workshop consisted of senior management and the project worker and focused on covering the status of the case project as well as the direction of the case project. The external workshop consisted of senior management, the project worker and an external consultant. During these workshops the external consultant shared information in regard to KATAKRI and the created material was reviewed and actions based on the results were decided.

4.3 Interview

Interview was used during the case project to define what are the expected results and how these results will be achieved during the project. Interviews were semi-structured and created a dialogue between the interviewer and interviewees. Through this, the author got Arctech's point of view into the project.

Interview was used to define certain problems that had risen during the case project. Interviewing was conducted in semi-structured sessions where the interviewer described the state of the project and the problem that existed regarding the project. At this point the interviewer asked for an opinion on the matter from the interviewee. Through free-dialogue interviewing it was possible to cover multiple topics in one sessions and sometimes this opened new questions in relation to the original question, that the interviewee had not thought of previously.

4.4 Case project

To show how the case project went and the major events during it the project is opened in STEPS (all of the STEPS refer to Figure 1). From these the recommendations for simplifying the KATAKRI preparation process are given in section 5.1. The STEPS part only covers the actions and processes done during the case projects. It will not go in detail in any documents that were created during the case project. The reason for this is to avoid leaking of classified material/information.

The case project had recurring processes so in order to avoid repetition during STEPS, the repeated parts (Preparation of material and checking /evaluating them) are shown in picture below Figure 7. These STEPS have some different actions but the core function (material creation) will refer to the set figure. This material creation process will be used in steps six, eight and eleven. Further information how material creation process has been used during this project is described in text below, when project steps are described in detail.

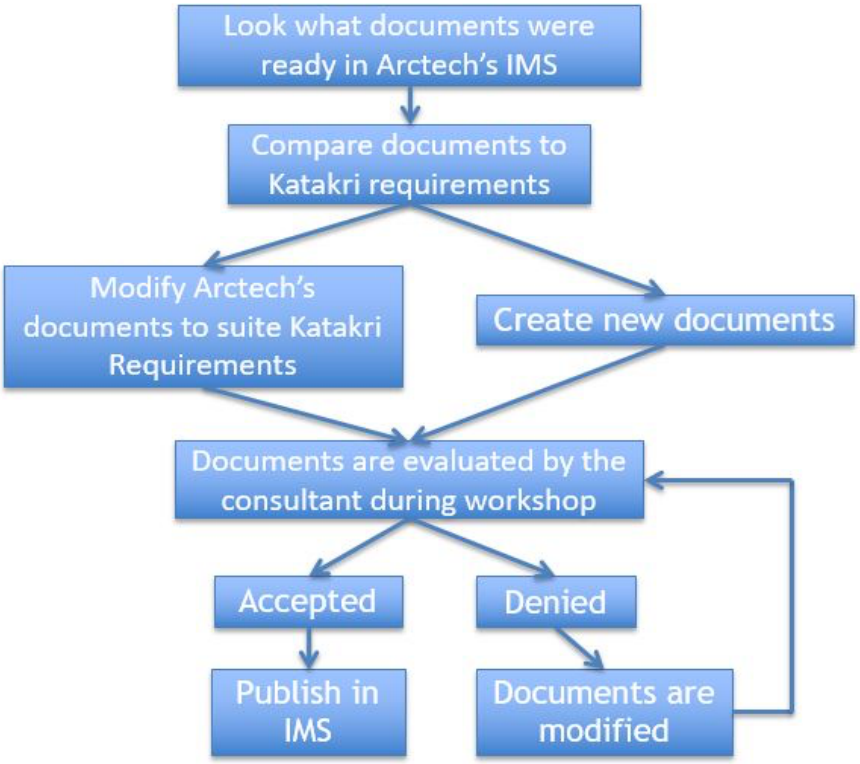

Figure 6 Creation of material and checking process

A) STEP ZERO

At the beginning Arctech had two choices concerning the project. First one was to apply for KATAKRI qualification and proceed with the project. The second option was to find find another way to develop information security (possibly different standard). Therefore, this was the first exit point. Arctech decided to proceed with option one, which led to hiring a worker for the KATAKRI project. A consultant was also hired to support the project.

B) STEP ONE
The existing company material was reviewed and the background for the project was collected. This included studying the KATAKRI tool. The reason for this was that fact that the project worker was inexperienced in using the KATAKRI tool. (This part can be described as self-study regarding the KATAKRI tool and the case project).

C) STEP TWO
An opening workshop was held. In this workshop all the parties that were going to be working on the case project met for the first time. This workshop group consisted of the CEO, the Heads of sales, ICT, production, design, HSE, HR, maintenance, plus the project worker and Consultant. Through this the workshop had parties from all the core functions of Arctech and support from a KATAKRI specialist (consultant). The topic for this workshop was: what the KATAKRI tool is, where it is based and how having KATAKRI certification benefits the company. This was the most important workshop of the case project, because through this, all parties of the project had a mutual understanding of what we are doing and why. At the end of the workshop Arctech had two options; the first one was to proceed with the project and proceed with preparing the material. The second was to cancel the project. This was the second plausible exit point.

D) STEP THREE
Preparing material for the Security Management part. This consisted of comparing Arctech's existing materials and company policies with the requirements set by KATAKRI. Purpose of this comparison was to find a solution that fulfils KATAKRI requirements but also still represents Arctech's company policies. To cut the workload, it was decided to use existing documentation as the basis for the new documents. This allowed quicker working and at the same time kept the creation of completely new documents to a bare minimum.

E) STEP FOUR
The first Internal meeting was held. Participants during this workshop consisted of the project worker and Arctech's senior management. The aim of this meeting was to be a preparatory meeting for the next workshop with the consultant. During this workshop, completed work was explained and the next step of the project was discussed.

F) STEP FIVE
The second external workshop was held. The participants were the same as the first workshop (project worker, senior management and consultant). During this workshop, the material consisting of company policies that was created between the workshops was evaluated by comparing them with the KATAKRI requirements. The consultant gave feedback on how well the created material fulfils the KATAKRI requirements and what should be changed so that documents cover the necessary requirements.

G) STEP SIX
Material creation continued based on received feedback from the consultant during the second external meeting. During this STEP the material creation process (Figure 7) was used for the first time. From this point on the material creation followed previously mentioned process.

H) STEP SEVEN
The third external workshop, with the same participants as previously. During the workshop material that had been created were evaluated and consultant gave feedback on how well they fulfil requirements. Also, previously evaluated policies were re-evaluated and accepted. During this workshop the decision to start preparing material for the Physical security part was made.

I) STEP EIGHT
Material preparation continued. (Following material creation process Figure 7) Accepted documents were implemented in Arctech's Information Management System (IMS) and rejected documents were re-evaluated and modified based on the feedback from the workshop.

J) STEP NINE
The second internal meeting was held. Participants were the project worker and Arctech's senior management. The focus of the meeting was to explain the status of the project and to further discuss where the project was heading.

Based on information given in this workshop the decision was made that the focus should be on finalizing the Security Management part documents and later evaluate should Arctech continue the project. As a result preparing material for Physical Security was halted.

K) STEP TEN
The fourth external meeting with the consultant was held. Created materials were evaluated again and based on the feedback they were either accepted or rejected. The workshop group consisted of the project worker, senior management and the consultant.

L) STEP ELEVEN
Material preparation continued. Accepted documents were implemented into Arctech's IMS and rejected documents were re-evaluated and modified based on the feedback following material creation process (Figure 7)

M) Step TWELVE

Arctech had two choices; continue to the Physical Security part and start investing in and constructing the necessary facilities or cancel the project. It was decided that the project be halted. Using the third exit point of the project.

The reason for using this exit point was to save costs. Because this project was not seen as mandatory it was decided that instead of investing more money in it, more crucial projects could receive funding. Arctech did not want to abandon the case project completely so they made sure that it was ended in a state where it will be easy to continue later in the future if they so choose.

At this point most of the Security Management parts documents were prepared to the extent that they could be implemented into Arctech's information management system (IMS) and used as part of the organisation's instructions. In that sense this was also an ideal exit point, because if Arctech chooses to continue the project at a later date they have the Security Management part ready and the project could continue on preparing Physical security and Information assurance immediately. Because the Security management was done, Arctech has the benefit of using these created tools as part of its daily operations and they may lead to further development of operations.

5 Results

The result section is a collection of findings that were made during the case project. Results are divided in two categories: general findings regarding KATAKRI (Section 5) and development recommendations regarding the KATAKRI preparation process (Section 5.1). General findings came from comparing existing KATAKRI material to the work made during the case project (Using theory in a real-life situation).

Firstly: KATAKRI treats protection of information as a whole, and therefore it is divided in to different levels of organization, dividing measured aspects on the sub-divisions Security Management (T), Physical Security (F) and Information Security (I). The foundation of KATAKRI is based on national and international legislation regarding information security and protection of data. With this KATAKRI can ensure that requirements are in line with national/international legislation and EU members' jointly made agreements.

Secondly: There are regulations that collectively give direction on how nations should modify their legislation. A good example is the EU regional regulation on information security, which states the guidelines on what the minimum requirements for national legislation are. With this the individual nations can update their own legislation regarding information security to be at the same level as the EU. This unified regional or "federal" model guarantees that even

if there are differences between the nations' laws, they should be in line with each other's and therefore they can be compared as such.

Thirdly: The difference between KATAKRI 2015 and KATAKRI 2011 is that the 2015 version is lacking information and concrete instructions for the person who is building the material. The 2015 version "*suggests*" what are the necessary requirements for certain security level compared to KATAKRI 2011 that "*states*" what are the minimum requirements on each level and what are the actions necessary for that certain level. This takes effectiveness from the person who prepares the material because they must really know what the necessary documents and actions are that are necessary to fulfil KATAKRI's requirements.

KATAKRI 2015 was modified to be the lighter version of criteria, narrowing requirements from 160 to just only 40. KATAKRI 2015 is content-wise almost identical to the older version but it combines requirements so that they became sub-requirements. This was achieved through combining requirements, and the idea was that this improves the usefulness of KATAKRI. The benefit of this structure is that it gives more flexibility to interpret requirements.

Of course, development and improving old criteria is necessary, but it should not lead to the above-mentioned situations. Many have criticized KATAKRI 2015 on these changes because they leave too much room for interpretation and praised the simplicity of KATAKRI 2011 because of the checklist nature that is easy to follow. The reason for this change was due to the Ministry of Finance wanting to develop this tool so that it will stand the test of time.

Fourthly: KATAKRI is in simple terms management of corporate security that has the goal of ensuring data protection. This is achieved with unifying regulations so that every user has the same measures in place and a unified scale of organizational security levels. KATAKRI is also meant to act as a guide to all users to develop internal security. KATAKRI tries to encourage companies to think of security as a concept that supports all sectors. This is creating a situation where companies recognise the value of security as part of their business values, rather than as a necessary expense or burden.

This situation was recognised during the discussions and workshops with the case company (Arctech). Through KATAKRI the idea that security should be a visible part of the company's daily routines instead of being a single entity within the company that is not connected to other actions. This broadens the security culture to the whole company, meaning that security must be visible; all the employees must be aware of security instructions and follow those rules. It would be beneficial for Arctech if the whole organization acts as a part of security. This also increases the customer's view of Arctech as reliable business partner.

Fifthly: During the case project, it was noted that the document updating process is slow and time consuming; it was crucial to use practical approaches. This means that the documentation has to withstand time so that they are still valid even after a longer period. In some documents this rule did not apply, for example documents that describe specific standards and specific products. This was due to that fact that the standards may change rapidly, therefore there must be changes so that the documents are up to date at all times. The project of updating documents is a continuous process. Affecting factors are for example the continuously changing standards and criteria.

Sixthly: When it comes to the visibility of KATAKRI standardisation in other companies, many Finnish companies show on their web page that they have the capability to undertake projects that need security clearance. Companies also state what is the highest level of material (based on KATAKRI) they can accept. By showing openly that the company has the capability to protect information of a certain level, customer interest in conducting business with said company will increase. This is due to that fact that information has risen to being one of the most important assets that companies have.

Seventhly: Having a KATAKRI certification would mean that Arctech has the capability to participate in projects between Arctech and EU/NATO members and is able to protect information belonging to these parties. It must be noted that going outside of the two regions/partners, it is wise to remember that legislation may vary depending on country. In these cases, it must be considered if the requirement set by the KATAKRI certificate is enough or is their need to increase the security of information. Because of this factor, caution must be exercised when determining the protection of information.

Eighthly: What was learned from the Arctech's case project was that the costs of a KATAKRI project depend on many factors. Costs divide into two main categories planning and building.

Planning includes the cost of preparing the material, the salaries of specialists that might be involved and administrative fees. Building costs come from facilities that are designated as areas where security classified material can be processed. To lower these costs, it is important to pre-plan properly what is necessary for the company and the project. The first thing is to plan how the material is prepared, how many workers are collecting and writing material and are there any outside consultants used. In some cases, it could be beneficial to outsource Katakri to ramp-up the process. With this the costs and time of the Katakri project budget can be forecast in advance. In a project that is made by the company itself, the costs can vary significantly from project to project.

The second thing is what kind of secure facilities are necessary for the company. For example, planning KATAKRI security facilities includes how many employees use the room, leading to how big the room must be and what sort of work is done in there. These factors define what kind of equipment must be in the room. There must be a well-made site plan for a security room and typically these plans are produced by an outsourced specialist.

It must be clear what is the decided security classification of the secure room leading to what kind of security system must be in place. At this stage it must be clear how the security room is managed. Because KATAKRI criteria sets different requirements for different security levels the types of facilities can differ tremendously. The facility can be as simple as modified office room or completely isolated room that is built inside of a Faraday cage. The facility can appear like a normal room, but the security level determines how the room has been built. In some cases, the security room can be outside the company's immediate premises.

5.1 Recommendations based on the case project

These recommendations are based on findings that were made during the case project. From these findings a framework to simplify preparation of KATAKRI's part T (Security Management) process was created. This also gives an idea of how the process works and what should be changed to have better results and improving the overall process. (The simplified version is shown in figure 8)

A) STEP ZERO
During this step it is good to examine alternative standards and compare them to the required end result. This action shows if there is an alternative way to improve information security within the company. Based on the case project and its objectives, KATAKRI was the right choice for a large company such as Arctech. Through this standard, Arctech would have had the competitive edge over other shipyards that do not have this level of information assurance, and it might also have brought work from customers that Arctech was unaware of.

B) STEP ONE
It was noted during the case project that reviewing existing material is crucial, because this gives a foundation on what the focus areas should be and what is the current state of the documentation. One major change to this STEP would have been the creation of a dedicated workgroup (Composition shown below) for this project. This change would improve overall productivity of the project, due to the fact that project workers could focus solely on the creation of documents and systems leaving the reporting to a dedicated individual. This also cuts the need of senior-management-heavy workshops.

Based on the case study the following composition of a dedicated workgroup is recommended: A Project Manager to be appointed leader of the project, the responsibilities of this person would be managing the project and informing senior management of the progress of the project. Working under the project manager would be 2 or 3 project workers focusing on creating materials. These workers' skills should complement KATAKRI subdivisions Security Management (T), Physical Security (F) and Information Security (I) bringing their special knowledge to creating documents.

C) STEP TWO

Having an informative meeting at the beginning of the project is vital, because it explains the project's agenda, what type of tool is to be used and what the company is trying to achieve by applying this type of standard. The reason for this is to get all participants on the same level of understanding of the project. The first workshop also gives the company the option to have an exit point at the beginning of the project if it seems that KATAKRI is too heavy for the company.

D) STEPS THREE TO FIVE

During these steps work consists of preparing the material, revising it with the consultant and internally with the workshop group. To make these steps more efficient the following improvements are suggested:

Preparing the material: The process used to create material (shown in figure 7) for KATAKRI can be used during this part. By using a set process in combination with the dedicated workgroup from STEP 1 the creation of material will be more efficient because more subdivisions can be tackled in the same time what broadens the material that can be created in a single preparing phase.

External workshops: Using a consultant or person with previous knowledge during this part is vital. This is because KATAKRI leaves room for interpretation and to ensure that created documents are in line with stated requirements it is necessary for a person who is knowledgeable in these matters to check created material with. Using experienced help also guarantees that created material is what the auditor might expect when the auditing phase starts.

When it comes to the composition of these workshops, the participants could be limited to the project manager, project workers, consultant and such managers as necessary for the topic the workshop is focusing on. This removes the need to include all department managers in all the workshops, which means organizing the workshops should be more manageable.

Internal workshops: These types of workshops should be status meetings with senior management. During these workshops the project manager can advise on the status of the project, the problems the work group has faced and what can be expected to be ready by the next meeting. By using this type of status meetings senior management will be constantly informed they have the possibility to ask questions regarding the project. These meetings can be also used to make decisions that need senior management's approval, for example if the project needs budgetary approval.

Internal workshops are also excellent exit points for the company: if the company sees that there is a need to cancel the project during these workshops, the company has the option to do so and set the time by which the project is run down reasonably. This means that the project should be cancelled so that there is a clear end point where the project can be continued from if the company so chooses in the future.

E) STEP SIX

During this step the company can end the project if they so choose or continue to the next step, which is the preliminary audit. This ensures that work is monitored throughout the pro-

ject and the company has the option to cancel the project if they so choose at any point in the project.

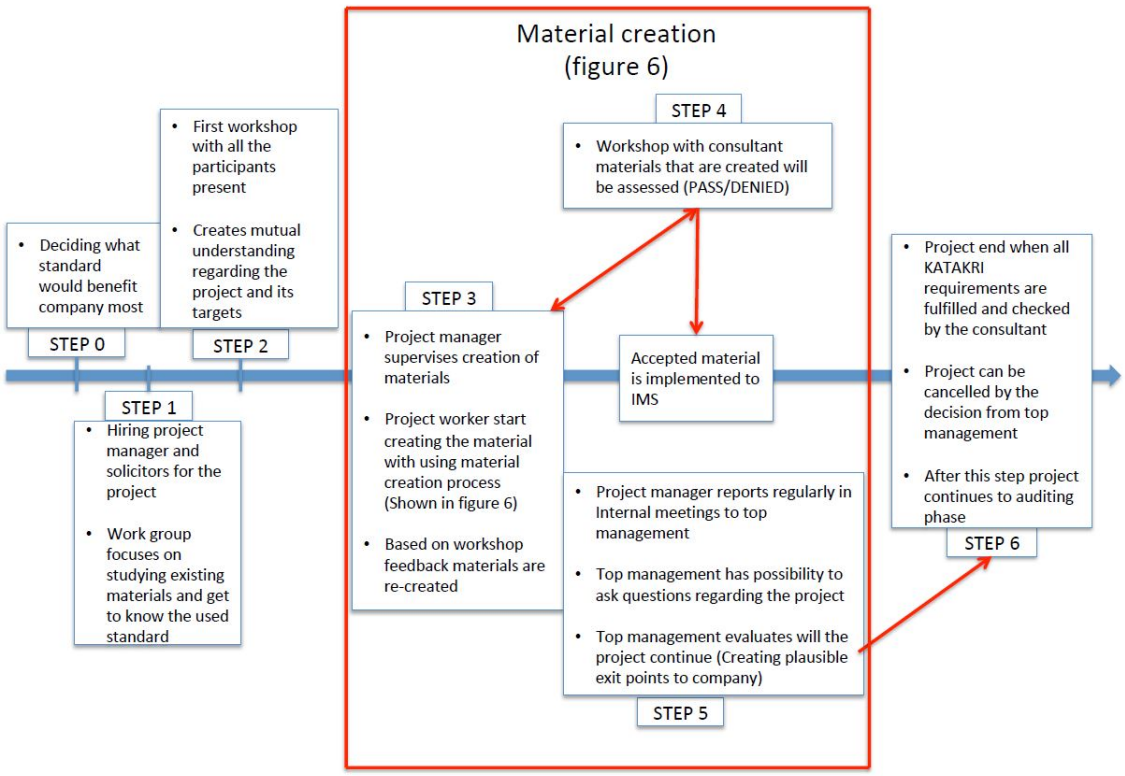

Figure 7 Simplified KATAKRI process

Figure 8 is a representation of the steps that are stated in section 5.1. The model simplifies the process used during the case project (Figure 1). Figure 8 model places the emphasis on dividing specific roles that enable a more focused way of working. Through using this model, the work can be done in a more efficient manner. Based on the case project modifying the way of working to follow figure 8 would be the “ideal” way of working because it removes multiple unnecessary actions and simplifies the whole process.

5.2 Objectives of the thesis

The objectives set for this thesis stated previously during the introduction (Section 1) were all covered and achieved during this thesis. It is recommended that this thesis be covered as a single entity, because this will give better a grasp of the topic.

6 Conclusion

Considering overall security is important, because if a company focuses on one single part of security, it leads to a situation where the overall security is unbalanced. By considering all sectors of security company ensure that the operating environment would stay secure and that a risk of something happening would be lower. This kind of behaviour also ensures that nothing is overlooked.

It was noted that it is beneficial for the company to be active in applying level of standards even though they are not applying one. By being proactive on seeking level of standard the company prepares themselves to operate on certain level of maturity by default. Also, company can apply standardization if they so choses more easily.

During the thesis, the finding was that for the next KATAKRI update there is a definite need to update requirements so that they are specific and clear for different security levels. This eases the workload of project workers and reduces the possibility for misunderstanding of the KATAKRI criteria. This eases the preparation process because the material is faster to create, therefore companies' average approval process time goes down. Quicker work leads to quicker end results and for this reason the KATAKRI process must kept as simple as possible.

Normally the KATAKRI preparation before preliminary audit takes time from half a year to a year. In these cases, material is prepared so that the level in preliminary audits is at the level of official auditing. Through this there is the possibility to fix detected deviations giving the best result for the final auditing.

There are some cases where the preparation process has taken more than a year. In these cases, the final audit has been delayed significantly. The delays came from the unwillingness of senior management to commit to security culture changes that are necessary to fulfil KATAKRI requirements. For this reason, it is crucial to have the full support of the company's senior management.

Having KATAKRI certification would open new business possibilities with the Governmental clients in Finland, but also would create possibilities to ensure internationally clients that the information is handled in a similar manner as Finnish Government would handle the information.

Through this thesis work the concept of information security was managed to introduce to Arctech's management supporting processes. Before this security was part of work health, work safety, and environment and the focus was on occupational aspects. With this work, we managed to balance the situation so that Arctech started to have security and information security as a visible part of the supporting process within the company.

The simplified version of the KATAKRI process introduced in this thesis (Figure 8) can be used if Arctech decides to continue applying the standardisation later. Through this, Arctech

should be able to continue work from the point where the case project ended more efficiently. Other companies that might consider applying for KATAKRI can use this model as a framework for reaching compliance.

6.1 For future development

For future development ideas for Arctech, one could be planning and creating a system that supervises continuity within the company. This means that all the necessary key resources, partners, suppliers and sub-suppliers would be recognized and that all parties are committed to Arctech's overall security culture. Business continuity should be ensured if something unexpected happened. Mapping these important parts of Arctech's business can be done as a part of risk management. Business risk can be then decentralized to a wider foundation.

For the future, it would be beneficial to study the shortcomings of KATAKRI 2015 compared to KATAKRI 2011. Through developing these qualities, it would lead to an increase of usefulness of this specific criterion. This work could be done in co-operation with the KATAKRI authorities so that the end result would be a manual for KATAKRI that can be shared with companies that might consider applying for KATAKRI.

6.2 Validity

The major part of the thesis and the project itself was done using data research. Because of the nature of the project being a case study, this was the most suitable method to carry out both of these tasks. All the thesis information for theory and methods was collected from multiple national and international authorities and peer-reviewed authors. The consultant then inspected all created documents that were related to the project.

References

Printed

EU council. 23 September 2013. Council decision on the security rules for protecting EU classified information (2013/488/EU). 15.10.2013. Official Journal of the European Union. Accessed 3 January 2017.

Heikkilä, H. 2004. Laatu ja ohjelmistotekniikka laatujärjestelmät. University of Jyväskylä. Accessed 28 December 2016.

Hirsjärvi, S. Remes, P. Sajavaara, P. 2013. Tutki ja kirjoita. Bookwell Oy. Porvoo. 2013

Jesson, J. K. Matheson, L. Lacey, F. M. 2011. Doing your literature review. Traditional and systematic techniques. London: Sages publications.

Kaunanen, J. 2012. Kehittämistyö opinnäytetyönä, Kehittämistutkimuksen kirjoittamisen käytännön opas. Tampereen yliopistopaino Oy. Tampere. 2012.

Kohnke, A. Shoemaker, D. Sigler, K. 2016. The complete guide to Cybersecurity Risks and Controls. CRC Press 2016.

Merna, T. Al-Thani, F. 2008. Corporate Risk Management. John Wiley & Sons Incorporated 2008.

Swanborn, P. 2010. Case Study Research: What, Why and How? SAGA Publication Ltd. 2010.

The Security Committee. 2015. Secure Finland, Information on comprehensive security in Finland. June 2015. The security Committee.

Electronical

Arctech Helsinki Shipyards. 2016. Background information. Arctech Helsinki Shipyards Inc. Accessed 12 December 2016.
http://arctech.fi/about-us/

Disterer, G. April 2013. ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security. April, 2013. Accessed 20.January 2018.
http://file.scirp.org/pdf/JIS_2013042311130103.pdf

Edwards, R & Holland, J. 2013. What is qualitative interviewing? Bloomsbury. London. 2013. Accessed 27 January 2017. http://eprints.ncrm.ac.uk/3276/1/complete_proofs.pdf

EK. 31 July 2015. Turvallisuusviranomaisten käsikirja yrityksille: Yritykseen kohdistuvat tietoturvallisuusvaatimukset turvallisuusluokiteltua tietoa sisältävissä hankinnoissa. Elinkeino elämän keskusliitto. Accessed 17 January 2017. https://ek.fi/wp-content/uploads/Turvallisuusviranomaisten_kasikirja.pdf

EK. 2017.Mitä on yritysturvallisuus. Elinkeinoelämän keskusliitto. Accessed 16 March 2017.
https://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/

EU council. 27 September 2016. The general data protection regulation. 24 May 2016. European council. Accessed 18 January 2017. http://www.consilium.europa.eu/fi/policies/data-protection-reform/data-protection-regulation/

Finnish Communications Regulatory Authority. 2017. Information security services of the NCSC - FI. Finnish Communications Regulatory Authority 2017. Accessed 20 March 2017 https://www.viestintavirasto.fi/en/cybersecurity/ficorasinformationsecurityservices.html

Mason, J. 2002. Qualitative researching. SAGE Publications. London. 2002. Accessed 27 January 2017. http://www.sxf.uevora.pt/wp-content/uploads/2013/03/Mason_2002.pdf

Ministry of Defence. 2017. Functions and organisation of National Security Authority. Ministry of Defence. 2017. Accessed 20 March 2017. http://www.defmin.fi/en/administrative_branch/defence_security/international_security_cooperation

Ministry of Finance. 2017. Vahti-toiminta. Ministry of Finance 2017. Accessed 28 December 2017. http://vm.fi/vahti

Ministry of Justice. 2016. The Act on the Openness of Government Activities. Ministry of Justice 2016. Accessed 20 March 2017. http://www.finlex.fi/en/laki/kaannokset/1999/en19990621.pdf

Murto, C. 2011. Kansainvälinen turvallisuusauditointikriteeristö, Katakri II. Puolustusministeriö. 05.11.2010. Accessed 20 March 2017. http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

National Security Authority. 1 December 2011. Industrial Security Manual. National Security Authority. 1 December 2011. Accessed 15 February 2017. http://formin.finland.fi/public/download.aspx?ID=105265&GUID=%7BC69A1FAF-2AA8-480A-9097-F395EF59F739%7D

National Security Authority. 16 March 2016. Kansainvälisen turvaluokitellun tietoaineiston käsittelyohje. Ministry for foreign affairs of Finland. 16 March 2016. Accessed 17 January 2017. http://formin.finland.fi/public/download.aspx?ID=142360&GUID=%7B3601698A-FC0F-485C-84FD-C7CA32513D1E%7D

Police of Finland. 2017. Security clearances. Police of Finland. Accessed 3 January 2017. https://www.poliisi.fi/security_and_monitoring/security_clearances

Puolustusministeriö. 2015. Katakri 2015 Information security audit tool for authorities. Puolustusministeriö. 26.03.2015. Accessed 27 October 2016. http://www.defmin.fi/files/3417/Katakri_2015_Information_security_audit_tool_for_authorities_Finland.pdf

Puolustusministeriö. 2015. Katakri 2015 Tietoturvallisuuden auditointityökalu viranomaisille. Puolustusministeriö. 26.03.2015. Accessed 27 October 2016. http://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Finnish Security Intelligence Service. 2017. Facility Security Clearance. Finnish Security Intelligence Service. 2017. Accessed 25 March 2017. http://www.supo.fi/turvallisuusselvitykset/yritysturvallisuusselvitys

Taylor, D. 2007. The literature review: a few tips on conducting it. Health Sciences Writing Center, University of Toronto. 2007. Accessed 16 February 2017. http://advice.writing.utoronto.ca/wp-content/uploads/sites/2/literature-review.pdf

The Security Committee. 2015. Turvallinen Suomi, Tietoja Suomen kokonaisuusturvallisuudesta. June 2015. The security Committee. Accessed 15 March 2017. http://puolustusvoimat.fi/documents/2182700/0/Turvallinen+Suomi+-Tietoja+Suomen+kokonaisturvallisuudesta.pdf/66ce96cb-f25a-4080-aa25-4c0c60afc2ec

Valtiohallinnon tieto- ja kyberturvallisuuden johtoryhmä. 2016. Toiminnan jatkuvuuden hallinta Vahti 2/2016. Valtionvarainministeriö 07.06.2016. Accessed 27 October 2016. https://www.vahtiohje.fi/c/document_library/get_file?uuid=11459f91-91c8-4ebe-a34f-9d8d9bfc964c&groupId=10229

Figures

Figure 1 Overview of the case-project 8

Figure 2 Risk management process (Vahti 1/2017) 11

Figure 3 Content of general data protection regulation 16

Figure 4 Security clearance levels..... 18

Figure 5 The case project workflow process..... 19

Figure 6 Creation of material and checking process..... 22

Figure 7 Simplified KATAKRI process 31

Figure 8 Acting authorities of Finnish National audit Criteria (Industrial Security Manual, 2011)39

Appendix 1 List of abbreviations

EU	European Union
KATAKRI	Finnish National Security Audit Criteria Tool
EUCI	European Union Classified Information
FSC	Facility Security Clearance
DSA	Designated Security Authority
NSA	National Security Authority
FSIS	Finnish Security Intelligence Service
DCF	Defence Command Finland
FDF	Finnish Defence Forces
GHQ	General Headquarters
NCSA	National Communication Security Authority
SAA	Security Accreditation Authority
NATO	North Atlantic Treaty Organization
HSE	Health, Safety, Environment
HSSE	Health, Safety, Security, Environment
GSA	General Security Agreement
NCSC -FI	The National Cyber Security Centre Finland
FSC	Facility Security Clearance
VAHTI	The Government Information and Cyber Security Management Board
IMS	Information Management System
ISMS	Information Security Management System
TEMPEST	Protective measures over hazardous diffusive radiation

Appendix 2 Acting authorities of KATAKRI

This part opens the whole KATAKRI organisation (also known as National Security Authority organization) to the reader. Through dividing jurisdiction and responsibilities, the organisation can focus on necessary tasks and all parties have a clear vision of what tasks they are responsible for. The responsibilities of this organization are to ensure that everybody (state, citizens, industries and communities) has the possibility to participate in international cooperation that contains classified material. This organization is also responsible for secure handling of foreign classified information. (Ministry of Defence, 2017)

During the case project it was necessary to understand which authority handles which part of the organization. This was because if the project had reached the implementation and auditing phase the respective authority would have conducted specific actions dedicated to them (see figure 5).

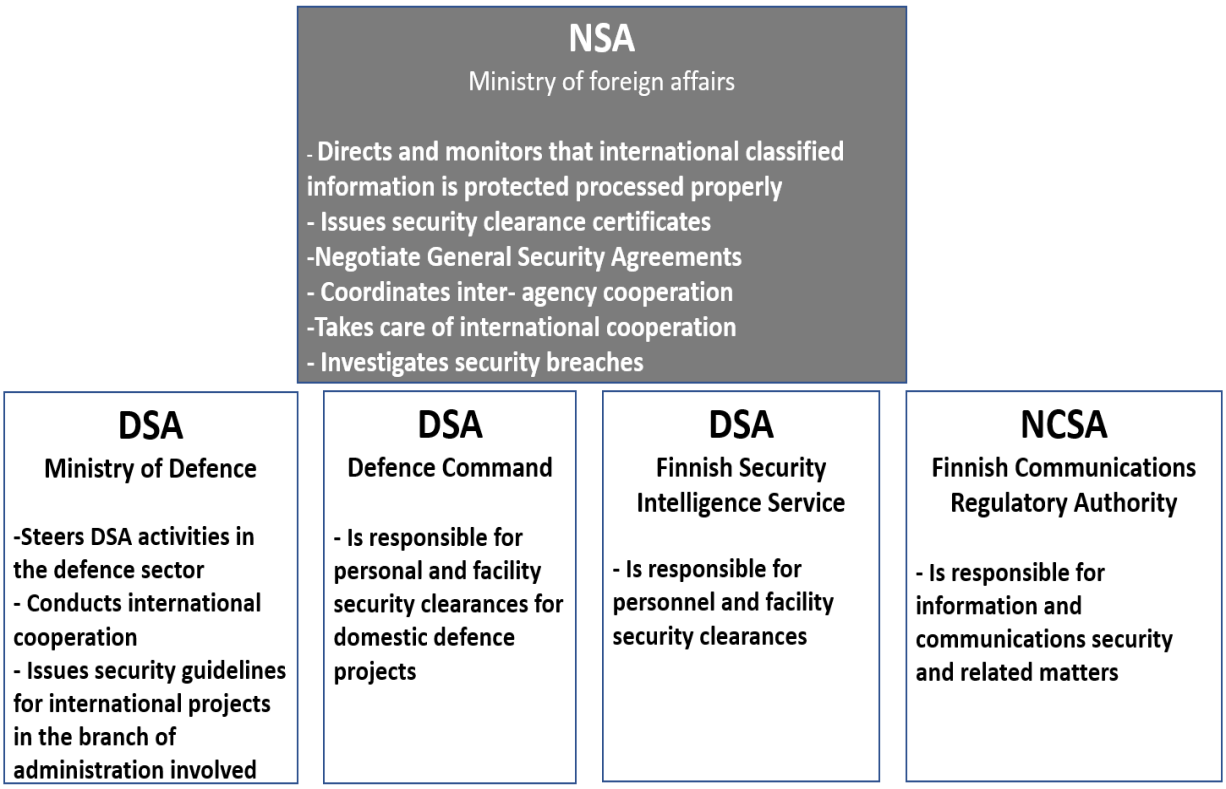

Figure 8 Acting authorities of Finnish National audit Criteria (Industrial Security Manual, 2011)

National Security Authority

Pointed as the National Security Authority (NSA) in Finland is the Ministry for Foreign Affairs. NSA is responsible for guiding procedures (based on obligations laid in Act of international information security responsibilities (588/2004)), preparing and negotiating General Security Agreements (GSA) and supervising that internationally classified information is protected and handled according to all binding agreements. (Ministry of Defence, 2017)

Finnish Security Intelligence Service

Law on security clearances (726/2014) states that: Finnish security intelligence service (FSIS) is the acting authority that has general jurisdiction to decide on conducting security clearances. FSIS decides on personal security clearances and facility security clearances unless the tasks belong to general headquarters of Finnish Defence Forces (FDF).

Finnish security intelligence service acts also as designated security author (DSA) and as specialist of national security author in execution of international information security obligation especially regarding personnel security, company security and premises security. (EK, 2015)

Defence Command Finland

Defence Command Finland (DFC) decides on conducting facility security clearances on industries that is intended to manage projects in Finnish defence forces (FDF) or on a company that is involved in procurement for the FDF. General headquarters (GHQ) decides to conduct a personal security clearance when the aim of the subject is to work in FDF, handle tasks given by the FDF or if the security clearance affects the actions or procurement of FDF.

GHQ acts also as designated security author (DSA) same as Finnish security intelligence service (FSIS) in fulfilling international information security obligations. (EK, 2015)

Finnish Communications Regulatory Authority

National communication security authority (NCSA) in Finland is the National Cyber Security Centre Finland (NCSC-FI). This authority is responsible for monitoring security measures (data transfers and data processes) regarding the protection of classified material. NCSA is also responsible for guiding and providing measures to protect classified materials within Finland. (Finnish Communications Regulatory Authority, 2017)

Ministry of Defence

The Ministry of Defence acts as the designated security authority (DSA) and takes part in international co-operation as the specialist of NSA. In addition, the Ministry of Defence accepts security documents regarding international projects and instructs creation of them within its administrative sector. (EK, 2015)

For understanding how the KATAKRI works it is important to understand who are the authorities behind it. This need can be seen for example when creating process documentation for the personnel background checking. Without knowing that the FSIS handles general background checks and FDF handles all matters related to defence field would lead to a process that is invalid.