jamk

Challenges of security classified projects from an IT management viewpoint

Marko Lehtinen

Master's thesis
April 2023
Technology
Master's Degree Programme in Information Technology, Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Lehtinen, Marko

Challenges of security classified projects from an IT management viewpoint

Jyväskylä: JAMK University of Applied Sciences, April 2023, 52 pages

Master's Degree Programme in Information Technology, Cyber Security

Permission for web publication: Yes

Language of publication: English

Abstract

The rapid rise of security classified projects in engineering and designing creates new challenges for IT management. Moreover, the world has changed a lot in recent years. For example, there is a war in Europe, and cyber security is more important than ever, which means security classified projects are more important than ever. The subject of the research was to study these challenges from cyber security and IT-management viewpoint. Company X ordered the research topic, which was done for their staff. The research was done primarily on the Finnish national level.

The research objective was to find challenges in classified security projects and the reasons for them. Identifying these challenges will help to organise these types of projects better and gives background about costs. Furthermore, streamlining the project workflow will help staff understand cyber security regulations better and make security classified projects more efficient.

The purpose is to give an overall picture of challenges for Company X and other companies that do security classified projects. It will also provide more information about IT cost structure. Which will help make better offerings for security classified projects. The research used the qualitative research method in the form of a questionnaire and semi-structured interviews to map the obstacles in these specific projects. Usually, costs and difficulties with the requirements cause challenges.

According to the research most significant issues are with instructions, education and guides for staff. Also, katakri regulations, especially in TL III projects, cause problems with modern software because network connection is not allowed. Furthermore, the author created recommendations for improving security classified projects.

Keywords/tags (subjects)

security classified, katakri, cyber security, cybersecurity, projects, IT management

Miscellaneous (Confidential information)

n/a

Contents

Figures

Tables

Acronyms

GDPR	General Data Protection Regulation
ISO 27001	International Organization for Standardization, Standard number 27001
IT	Information Technology
KATAKRI	Kansallinen turvallisuus auditointikriteeristö, Information Security Audit Tool for Authorities
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
NSA	National Security Authority of Finland
PCI DSS	Payment Card Industry Data Security Standard
SANS	SANS Institute, officially the Escal Institute of Advanced Technologies
TL II	Turvallisuusluokka II, Security classification class II
TL III	Turvallisuusluokka III, Security classification class III
TL IV	Turvallisuusluokka IV, Security classification class IV
VAHTI	The Government Information Security Management Board

1 Introduction

The research is being done because the challenges of security classified projects interested Company X, the orderer of the work. In this thesis, secure or classified projects mean security classified projects regarding the Finnish government classification called Katakri, various types of security specifications or some other classification by the ordering client of the project. These projects can be, for example, engineering planning, software development, or many different projects. The common thing is that they are classified, and often Finnish government is the client for the projects. VAHTI is security guidelines created by "the government information security management board". Therefore, VAHTI information security instructions are often mentioned as security guidelines in security classified projects. Katakri (*kansallinen turvallisuus auditointikriteeristö*) is a tool used to audition these classifications (Ulkoministeriö, 2021a). A *project* is a task or activity completed over time to achieve a specific goal (Cambridge University Press, 2022).

The thesis will focus on security classified projects' cyber security and IT management challenges, especially software development and engineering planning, especially on Company X's experiences with security classified projects. These projects are extremely challenging from an IT management perspective. Moreover, since Company X is an engineering company that mainly designs things, these issues usually delay the projects or cause extra costs to them.

Katakri's requirements make the modern way of managing IT devices difficult. Katakri requirements cause issues that sometimes take work to solve. Often actual costs are much higher than the business units think. Security classified projects generate everyday challenges in the IT department and information management.

The research will use the qualitative research method, questionnaire, and semi-structured interviews to map the obstacles in these specific projects. Usually, costs and difficulties with the requirements cause challenges. For example, a typical challenge is software licensing. Most design software companies use cloud licensing or network licensing, where designers' computers need an internet connection. However, this connectivity is only allowed in some Katakri requirements, depending on the security level. Of course, the project's client can change the criteria, which is sometimes the case. Sometimes the requirements are changed by the client to accomplish the desired

outcome. The companies are also facing many other issues with these types of projects. For example, sometimes guides and instructions for users could be more precise.

This thesis can give an overall picture of challenges for Company X and other companies that do security classified projects. It will also provide more information about IT cost structure. Which will help make better offerings about these types of projects. Costs are calculated with estimates since the actual costs depend on many things this thesis cannot cover.

The thesis will not cover physical security, only when it affects IT or information management. Furthermore, cloud security is not covered since Katakri only sometimes allows network connections. Therefore, this thesis will focus only on Katakri classified projects, mainly on classification levels III (TL III) and IV (TL IV). These classifications will be explained in chapter 2. However, results can be, of course, used in any classified security project.

1.1 Company X

Company X, which has ordered this research, is an engineering company. Company X operates in building design, infrastructure design and digital solutions. All three business areas are engineering businesses. Even the digital functions that develop software and solutions. Company X is a company that works in project style.

Company X has thousands of experts who design cities, buildings and traffic infrastructure. Company X combines daily living with a durable foundation and tries to achieve a carefree everyday life. The company's head office is located in Finland. Company X operates also in Nordic countries.

Company X undertakes a considerable number of security classified projects annually in Finland, which has provided opportunities for the company to develop and enhance its security capabilities. Although the security requirements can make the work time-consuming and challenging, the company is committed to ensuring the success of these projects and overcoming any challenges that may arise.

1.2 Research objective

The research objective is to find challenges in security classified projects and the reasons for them. Identifying these challenges will help to organise these types of projects better and gives background about costs. Furthermore, the author hopes to analyse the issues deeper and create recommendations for improving security classified projects.

The research questions are:

- What challenges do security classified projects have from an IT management perspective?
- How can these challenges be solved?
- How do the costs of security classified projects compare to regular projects?

1.3 Research methodology

The type of research used in the thesis is by nature qualitative, and it uses the qualitative research method to map the obstacles in the specific projects discussed in the thesis. Therefore, the chosen research method can offer a broader view of the subject. The idea is to find all possible challenges and problems in security classified projects regarding IT management. Once the issues and challenges are known, we can better understand the quality and amount of the issues.

The qualitative research method is used to analyse the data gathered in two parts of the research. The first questionnaire is for the engineers and project managers working with security classified projects. This questionnaire includes scaled questions to determine the overall feel of the people working on the security classified projects and free text questions to get essential data and broad answers. Then, based on the answers, there will be a semi-structured interview with crucial personnel essential in security classified projects. In semi-structured interviews, closed- and open-ended questions are used, frequently with follow-up inquiries (Schmidt. 2004).

This second part of the method includes questions, and a semi-structured interview about IT costs in security classified projects with key persons. These cost-related questions will help the author

do the cost analysis to compare security classified projects to regular ones. These interviews were conducted in person or via Microsoft Teams. Again, these interviews were recorded and transcripted.

This type of research gives a broad aspect of the area and allows designers to point out challenges not foreseen by the author. Portney (2019) claims that the emphasis of qualitative research is on the opinions, conclusions, and conversations of professionals in the field of cyber security, their foundations, objectives, and implications with a broad analytical perspective.

1.4 Ethics

The thesis study follows the ethical principles of Jyväskylä University of Applied Sciences. Every attempt has been made to ensure that the original sources are acknowledged. There are no intentional violations regarding citations, reference lists, and the use of software licenses and apps. (JAMK, 2018)

The thesis does not publish personal information, and processing GDPR-compliant data was unnecessary for the research. Data collected include questionnaires and interviews. Raw data will not be published, only responses and results.

The author's work contract with Company X partly regulates the research integrity of the thesis. Therefore, the research data published in this thesis will be filtered. The names of designers and projects have been removed from the data gathered to protect Company X's customer trade secrets and contracts. In addition, all data that has been identified to be harmful to Company X or partners have been filtered out. Nevertheless, the results obtained from the research should be useful and accurate.

Costs are calculated with estimates since the actual costs depend on many aspects that this thesis cannot cover. These costs are taken from publicly available information to protect Company X and its partners.

All unpublished research data is deleted after publishing this thesis at the request of Company X.

1.5 Reliability

The reliability of the research was taken into consideration in all phases. The author delivered this thesis's data, results and drafts to Company X security personnel throughout the research. When creating the questionnaire, all questions were thought together with the Company X security personnel. Results are considered reliable since there is no foreseen reason for persons to lie or manipulate the results. Company X also trusts its employees. There is no reason to suspect any foul play on the answers. Reliability criteria used in qualitative research are reliability, portability, dependency, confirmability, and saturation. According to the reliability, the findings of the study are accurate (Kananen 2015).

Analysis of data is the author's perception. Even when trying to be objective, this can cause errors in interpreting raw data answers. Some simplification needed to be done since some of the responses were very long and complex. Overall, the reliability of the research is maintained because of the chosen methodology and since the amount of data is significant enough.

Semi-structured interviews are conducted to validate questionnaire results and get detailed background information about the subject.

1.6 Previous research

Security-classified projects have yet to see much research. It is difficult to find any literature on the research topic. Most books about cyber security in Finnish have used the same official Katakri document as a source. There are a few theses written about this topic. Usually, bachelor-level theses are about physical protection from the Katakri perspective. These theses can be found using “tietoturva luokiteltu” as a keyword in Open Repository Theseus - the theses and publications of the Universities of Applied Sciences on the Internet (Theseus. 2023). These theses focus on the

physical side of Katakri. They have not helped much in this research since physical security was outside the scope. Since Katakri is a national tool mainly used by the Finnish government, it limits the research. In some ways, this thesis is groundbreaking research. The author could not find any books about security classified projects made using Katakri. Unfortunately, this is a national-level tool, so international books about security classified projects do not give any insight into this thesis. It would also be outside the scope of the thesis. Due to the secrecy of the topic, it was also challenging to find other source material, e.g. journal articles.

Vaarasalo wrote a bachelor thesis about TL IV classified environment hosting multiple projects from the network perspective of TL IV projects. The result was audited and approved by authorities. It is an exciting paper for IV projects. Vaarasalo's research is an excellent background for security classified project networking (Vaarasalo, 2021). TL IV is the highest classification allowing network connectivity, according to Katakri (Ulkoministeriö, 2021a).

There is also another bachelor-level thesis about security classified construction projects written by Piiparinen. It is about how security classified projects' special requirements affect the actual construction of buildings. Furthermore, it gives exciting views of how security classified projects are performed. It offers an excellent overall read for the subject and provides a broader perspective (Piiparinen, 2021).

Tasala has written a bachelor's thesis in diary form. He worked as a project manager in security classified projects at Equinix. The thesis was about a security classified building project and presented a broad view of the subject (Tasala, 2020).

There is an outstanding amount of cyber security research about international auditing tools and standards such as the NIST Framework, PCI DSS, SANS and ISO 27001, which are widely used global standards and frameworks (Hibberd, 2022).

In Finland, the Government Information Security Management Board (VAHTI) publishes IT guidelines and instructions for government agencies and municipalities. This board has been around since 1992. These instructions also work in private companies and give excellent risk management and cyber security guidelines (VAHTI, 2023).

2 Background about security classified projects

In this thesis, all security classified projects are based on Katakri classifications. There is a security classification of information behind Katakri. In Finland, information security is classified into five levels (Valtiovarainministeriö, 2021):

- TL I Erittäin salainen. Top Secret.
- TL II Salainen. Secret.
- TL III Luottamuksellinen. Confidential.
- TL IV Käyttö rajoitettu. Usage Restricted
- Salassa pidettävä. To be held secret.

This information classification is behind Katakri. Katakri uses only three levels TL IV, TL III and TL II. Therefore, this thesis mainly focuses on TL III and TL IV projects. Sometimes private companies use similar classifications, but their regulations differ from Katakri.

2.1 Katakri

The abbreviated name Katakri stands for “Kansallinen turvallisuusauditointikriteeristö”. Which translates into English, Information Security Audit Tool for Authorities. Katakri is used to audit security arrangements and assess the security of authorities’ computer systems. Private companies use Katakri to improve data safety. By using Katakri we ensure necessary security arrangements to provide data integration and keep classified information safe in all environments. There is also a physical side in Katakri, which helps to ensure data information in the physical environment. Katakri works well on domestic and international projects. Katakri is a collection of minimum requirements based on legislation. The newest version of Katakri from 2020 is a guide with 116 pages, including its subdivisions for security management(T), physical security(F) and information assurance(I). Katakri requirements are named by subdivision and requirement number, for example, T-01. Katakri is also available in English. Katakri is the baseline for working with the Finnish government and ministries. Companies working with the government often go through Katakri auditions, where an external auditioner performs the audit. Katakri is a tool for regular times, and it has not been meant for exceptional conditions such as environmental disasters, war, or pandemic

situations, e.g. COVID-19. However, it can also be used in such situations as virus pandemics or military conflicts (Ulkoministeriö, 2021a).

Katakri has three security classification levels. Level 2 is the most secure.

- Level two: Secret. TL II.
- Level three: Confidential. TL III.
- Level four: Restricted. TL IV.

All these levels have different requirements for storing and accessing data. However, some mandatory requirements are the same for all levels—e.g., how a company identifies visitors in company areas and monitors their visitors. For example, there are requirements for security areas, soundproofing, protection from unauthorised observation and using courier services. There are also requirements for how data should be disposed of (Ulkoministeriö, 2021c).

Even though Katakri includes parts from cyber security frameworks such as NIST or SANS, its purpose is entirely different. Katakri is also unique work of the Finnish National Security Authority called NSA. There are only a few similar international auditing tools, most of which are based on NIST, SANS, and ISO27001 security frameworks (Ulkoministeriö, 2021b).

2.2 Katakri subdivisions

Katakri has three subdivisions that describe the requirements for Security Management(T), Physical Security(F), and Information Assurance(I). From an IT management perspective, all are equally important.

2.2.1 Security Management (T)

This subdivision covers methods and controls for implementing security management in the entire organisation. It includes administrative information security and personnel security. It ensures that

employees handle classified information correctly. Security management is the cornerstone of every organisation. These controls and methods should be focused on the part of the organisation that runs the security classified information. This part of Katakri is an essential part of proper risk management. All Katakri plans and instructions inside the organisation should be in written format. There are requirements for management(T-01, T-02, T-03, T-05), risk management(T-07, T-12, T-13), guidance(T-04, T-12) are personnel security(T-09, T-10, T-11) (Ulkoministeriö, 2021c).

2.2.2 Physical Security (F)

This subdivision covers methods and controls for physical security to prevent unauthorised access to classified information and ensures that data is secured enough to cover confidentiality, integrity and availability requirements. It provides methods to help design new facilities and protect existing facilities. The requirements in this subdivision need to be put in place as completely as possible. A sufficient level is always based on risk assessment. All security areas need to be audited. The auditor evaluates physical security and considers whether the risk is acceptable. There are requirements for security areas that include, for example, materials of walls, windows and doors(F-03, F-05, F-06). The requirements include other types, such as mandatory ID badges (F-05.2, F-06.2). Keys can only be handled by a person with access to secure areas(F-05.2, F-06.2), and visitors must be escorted at all times (F-05.3, F-06.3). There are also requirements for alarm systems(F-05.5, F-06.5), soundproofing(F-05.4, F-06.6) and electronic equipment inside the security area(F-05.7, F-06.9). This subdivision also has requirements about using postal or courier services, which often affect the IT department(F-08.1). For example, courier services are not allowed unless data uses strong encryption. (Ulkoministeriö, 2021c)

2.2.3 Information Assurance (I)

This subdivision covers methods and controls for Information Assurance, primarily affecting computer networks. This subdivision involves most IT departments' work. It includes some of the critical requirements such as the security of the network architecture(I-01), segmenting network(I-02),

network monitoring systems(I-03), management connections(I-04), wireless transmission(I-05), systems hardening(I-08), malware protection(I-09), event logging(I-10), incident detection(I-11) and backup copies(I-20) (Ulkoministeriö, 2021c).

2.3 IT Management

IT management refers to the processes and activities involved in overseeing and maintaining an organisation's information technology infrastructure. It includes hardware, software, networking systems, and the people and processes that support them. IT management is responsible for ensuring these systems run smoothly and efficiently and meet the organisation's needs. The monitoring and control of an organisation's information technology systems, including its hardware, software, and networks, is called IT management. IT management monitors and governs IT systems to guarantee consistency and dependability. Furthermore, it focuses on improving information systems' effectiveness (IBM, 2023).

IT management typically includes tasks such as planning, budgeting, and procurement of IT resources, managing software development projects, network and system administration, and providing technical support to users. It also involves overseeing the implementation of security measures to protect the organisation's information and systems from unauthorised access or damage.

In Company X, IT management makes working possible. IT management supplies users with software, computers, laptops and other devices. IT management also manages all enterprise networks and cloud services. IT management is the critical function towards digitalisation. IT is the core of many enterprise functions. One of the essential duties of IT management is to make working more efficient.

IT management protects the company from cyber risks by taking care of cyber security, backups and access rights. It is worth noting that Company X holds an ISO27001 certification, which serves as a testament to the excellent work done by its IT management team in ensuring robust

cybersecurity measures are in place. Although this certification may differ from the security requirements of security classified projects, it provides a solid IT management and support foundation.

IT management works closely with the business unit and security department in security classified projects. Making sure the actual design work is possible. Understanding KATATKRI, VAHTI, and other classifications are essential when working in Company X IT management and support.

2.4 Possible identified challenges

At this point, the author has identified the following challenges while working with security classified projects. These are the author's views about the challenges encountered. These identified challenges were identified before the research. The author is interested to find out how accurate these identified challenges are.

Customer agreements and Katakri require hardened IT management systems to save information about security classified computers. In a hardened environment, tools from a regular environment can not be used. This hardening might cause issues since IT management does not see these secure devices in usual device listings. In addition, it might cause issues managing devices, updates and other maintenance duties.

Sometimes, it is impossible to use courier services to move secure laptops between offices. Someone has to carry out the setup if the computer is being used in a project since there might be project data in the computer. Not using courier services is a problem since Company X have offices allover Finland. Also, the security of devices must be monitored when they are moved to other locations.

IT Support can not use remote connections to help users or set up laptops. In addition, all offices do not have local IT or IT personnel with security clearance. Updating devices and doing periodical

maintenance is also tricky. Working with hardened devices requires special knowledge and being on-site.

Applications can not use the internet or network connections to get license information for design software. Not having a network is a big problem. Autodesk does not offer offline licenses anymore. There are only network licenses that are difficult to get work in locally. There is the same problem with other design software, which causes extra costs. Also, some of the models needed in CAD work are easier to get on laptops with a network connection. Some of the regular features can not be used in a secure environment.

The costs of manually maintaining security updates for laptops are vast. In addition, updates are not monitored in real-time because the network is not allowed, so there might be un-updated devices in secure projects. That is not necessarily a risk since machines do not have network connectivity. Nevertheless, it is an issue, according to Katakri.

Gathering logs in real time from laptops is only possible with the network. As a result, logs are only collected when doing management duties with secure laptops. Because of this, log collecting is not real-time and needs manual analysis. It is also difficult to notice if the secure laptop is compromised with malware since modern malware can clear the log entries or turn off the logging.

Only named accounts are allowed on security-controlled computers. It causes issues where the computer is located physically in a different place than IT support which has the right to manage the security-controlled computer. The passwords of these local accounts are straightforward to forget. It causes extra work and costs.

3 Questionnaire

The language of the questionnaire was Finnish since that is the language of end users and used in Company X. Questions were finalised with the help of Company X security personnel. The questionnaire was conducted using Microsoft Forms. It is a cloud tool for questionnaires, surveys and

polls. Forms can output the results in a Microsoft Excel file. Which is a helpful feature when analysing the answers (Microsoft Forms. 2022).

Persons answering the questions were identified from internal project data and Company X security personnel. This internal data was unstructured, and raw date needed filtering. Project managers and persons working on less than five classified projects were filtered out. The questionnaire was sent to chosen persons in September 2022. The last date for accepting answers was the 1st of October—all questions required to be answered. There was a total of 33 responses.

After reading the responses, it was apparent that questions should have separated different security classifications, especially TL III and TL IV classifications. In the responses, users answered based on different mixed security classifications. This was an issue that the author or Company X's security personnel could not forecast. After careful thinking, it is clear that entirely different classifications should have been considered much better. For example, TL IV requirements are much simpler than TL III requirements. This slightly corrupted the data gathered. However, answers were mainly compatible with both conditions. Most of the challenges on these projects are the same in both classifications. Even though the author considers this a mistake, it gave good answers to research questions. Separating these into classifications would be essential, but since this research was also part of the user perspective, this did open that perspective more.

3.1 Questions translated into English

The questionnaire was translated from Finnish to English by the author. After the question, there is a method for answering yes/no, scale or free-text. Original questions in Finnish are located in appendix 1.

1. Have you done security classified projects? (Yes / No)

   The functionality of IT in security classified projects
   How well do the following areas work in security classified projects?
   On a scale of 1-5. 1=Really bad, 2=bad, 3=OK, 4= Good, 5=Excellent

2. Networks (On a scale of 1-5)
3. Software (On a scale of 1-5)
4. Computers (On a scale of 1-5)
5. The flow of work (On a scale of 1-5)
6. What challenges have you encountered in security classified projects? (Free-text)
7. How large would you estimate the IT costs of a security classified project compared to a normal project?
   (On a scale of 1-5)
   1=Significantly smaller, 2=smaller, 3=Equal, 4= Bigger, 5= Significantly bigger
8. How would you evaluate the use of working time in a security classified project compared to a regular project?
   (On a scale of 1-5)
   1=Significantly smaller, 2=smaller, 3=Equal, 4= Bigger, 5= Significantly bigger
9. Are the instructions and regulations clear in security classified projects?
   (On a scale of 1-5)
   1=Really unclear, 2=unclear, 3=OK, 4=A little to improve, 5=Perfectly clear
10. How could the instructions be improved?

3.2 Background of questions in the questionnaire

In this chapter, the author explains the background for selected questions and the reasoning behind the question. The chapter helps to understand the background of research and reasons better.

Question 1. Have you done security classified projects?

The first is a filtering question to ensure the user participated in a security classified project. This first question is essential since raw data used to map users participating in security classified

projects must be more accurate. The total number of responses was 33. Therefore, after filtering, the number of actual valid responses is 32.

Question 2. Networks (On a scale of 1-5)

This question is trying to determine how users feel about the functionality of networks in security classified projects. This question would benefit from separating TL III and TL IV classifications since networks are not usually allowed in TL III. One of the free-text answers to question 6. also pointed this out.

Question 3. Software (On a scale of 1-5)

The question aims to find the user's mood towards software solutions in security classified projects. There have been a lot of issues and challenges in IT management regarding software in security classified devices. With this question, the author tries to determine how the end user feels about the software's functionality on these devices. The question also tries to find an answer to whether the end-user or designer feels the same way as the IT management.

Question 4. Computers (On a scale of 1-5)

This question is trying to determine how users feel about the functionality of computers in security classified projects. Computers are similar hardware used in regular projects. There are only cyber security hardenings and some software differences. The end user might be unable to separate software and computer very well. Sometimes issues with computers are perceived as issues in software and vice versa.

Question 5. The flow of work (On a scale of 1-5)

This question determines how users feel about the flow of work in security classified projects. This is essential since higher results would mean happier and more productive employees. Suppose users think that the flow of work could be better. It will impact their motivation and happiness. Since

in security classified projects, the whole workflow is different to regular projects. Answers are a good benchmark of how IT management has succeeded overall.

Question 6. What kind of challenges have you encountered in classified projects? (Free-text)

The author hopes to get detailed answers that broaden the IT management insight. Since only some of the issues designers and engineers experienced have reached IT management. The author is optimistic that people answering the questionnaire share the same passion for fixing the issues and challenges. This question is the most important. A good analysis of the responses to this question is crucial for this study. The author should get much information about the challenges in security classified projects based on free-text answers.

Question 7. How large would you estimate the IT costs of a security classified project compared to a regular project? (On a scale of 1-5)

The question tries to determine how the designers feel about the cost of a security classified project compared to a regular project. While working in IT management, the author has noticed that engineers working on these projects often need to realise the actual costs. This might be because engineers need to learn the cost structure better. The author hopes to understand better if this is a real issue that needs to be clarified.

Question 8. How would you evaluate the use of working time in a security classified project compared to a typical project? (On a scale of 1-5)

The question determines how the designers feel about working time in security classified projects compared to regular projects. Of course, a worker's time always costs. This question tries to clarify whether the designers think working on security classified projects is slower or even faster than on regular projects. Based on these answers, free-text answers and interviews author hopes to find answers that help determine the costs.

Question 9. Do you feel the instructions and regulations are clear in security classified projects? (On a scale of 1-5)

The question tries to determine how the designers feel about the clearness of instructions and regulations on security classified projects. The author has noticed that sometimes engineers or designers need help understanding and internalising instructions and regulations with the security classified projects. The question explores how they feel about the instructions and regulations. Question 10 should give even broader answers to this question.

Question 10. How do you think the instructions could be improved? (Free-text)

The question explores engineers' and designers' ideas about how the instructions and regulations could be more precise. The author hopes to get diverse answers that broaden the reasoning in IT management. The author may even get some valuable suggestions. The question is essential for this study since it gives the engineers and designers a voice to give honest feedback. Based on free-text answers author should get much information about the issues in security classified projects.

4 Interview Questions

During January 2023, The author conducted interviews with Company X personnel. The method used is the semi-structured interview. The author used three specific questions. The goal was to get answers to those questions, validate questionnaire results and get detailed background for the research.

The interview involved three persons from Company X. CIO, Security Manager and Systems Administrator. These persons were selected because they have the most knowledge about IT management issues in security classified projects. As background information, they got questionnaire results to see before the interview, including questions to be asked. The author hopes to get better answers if the interview subjects have time to consider the responses. It also helps to verify and validate the questionnaire results. The author recorded and transcribed the interviews. The author reports the results of interviews in order of questions. The author combined responses into

a single, easy-to-read form. Three specific questions led to interesting conversations around the subject area.

- You saw a list of questionnaire results. Was there anything surprising in the user responses?

- What things do you see as the biggest challenges in security classified projects?

- About the costs. What things cause costs in security classified projects compared to a regular project? Can you estimate the sizes or euro amounts?

First question: You saw a list of questionnaire results. Was there anything surprising in the user responses?

All interviewed agreed that there were no big surprises in questionnaire responses. All of the issues designers reported have been in discussions before or acknowledged. Instructions and guides that need to be clearer are worrying since instructions are manifold, and the reader must want to understand them. Simplifying the instructions and principles is not possible after a certain point. All the security classified projects are different, and they have different requirements. It makes instructions and guides complex. Because projects are different, also instructions are different on all projects.

Sometimes customers need to classify the data correctly or know what the classification means. Customer requirements keep changing during the project. Sometimes they harden the requirements and sometimes loosen them. It causes ambiguity in the classifications. Ours and the customer's information security organisation are too far from the actual work. It causes misinterpretations and confusion. Requirements are often open for interpretation, and designers need to find clarifications. Sometimes security requirements are just stamped on the project without understanding why. The security classified project might get a higher classification; at some point, it is acknowledged that it is unnecessary in the project. There might be the case that there is no need to classify anything.

Modern designing software is not intended to work in an isolated environment without an internet connection. Even if we get the licenses to work, they are crude versions of our everyday tools, which change the workflow and make things extremely difficult for the designer.

Second question: What things do you see as the biggest challenges in security classified projects?

A change in operating methods takes time, and these security classified projects have raised the level over the last few years, so it will take time to happen. In the past, everything has been as open and public as possible. Everyone can work anywhere. People who have never used memory sticks come to work and must understand that Onedrive or cloud services cannot be used. Designers prefer to keep the way of working the same, and in security classified projects, the tools and the way of working change entirely. The workflow and operating methods are utterly different from the end user's point of view. The end user thinks this is an IT-management problem since this environment IT-management delivered. It is about managing the customer's risks and removing a vast risk vector when there are no network connections. It has an apparent reason for the security of the nation.

Maintenance of security classified devices is one big challenge. Devices need updates to operating systems, software and licenses. Sometimes there is a need to install new design software. These are difficult to handle since all the devices are all over Finland, and there might not be local IT support with security clearance available in all offices. Since there are no internet or remote connections to these devices, IT support needs to travel. It causes costs in the form of work time and travelling.

Getting a non-network license takes work. All design software relies on network licensing or cloud connectivity. Security classified devices do not have a network, so this is a big issue. For most, the design software can get the offline license, but they are often tricky to install and challenging to get. It usually takes two weeks or more to get the license. Most of the licenses are for one year. It is costly since sometimes actual design work might take for few weeks. To buy a license for a whole year is unnecessary for these projects. The security classified device might be unused in a safe for most of the year.

Third question: About the costs. What things cause costs in security classified projects compared to a regular project? Can you estimate the sizes or euro amounts?

The costs have multiplied precisely because of software licenses. It is because there are no licenses suitable for an isolated environment anymore. Depending on the software, the license costs can be multiple times higher than in regular projects using network licenses. Sometimes the security classified device is used for a week and then sits in the safe for the rest of the year. Actual hardware or installing the security classified device for usage is nothing special compared to a regular device. The device costs come from maintenance and IT support. IT support needs to travel all over Finland. It causes costs in the form of work time and travelling. Updating and installing security classified devices takes much time compared to regular devices. These IT support costs are multiple times higher than in regular projects. The minimum costs in security classified projects compared to regular projects are double since designers have device and software licenses for two devices—one for security classified projects and one for regular projects. This minimum is hardly ever achieved.

5 Analysis

In this chapter, the author tries to analyse the questionnaire and interview results. In free-text responses, the analysis is made by interpreting the answer. The purpose is to find specific issues, challenges and fixes for them. Free-text responses are summarised and counted based on similar answers. In scaled responses, there is more mathematical analysis involved. In scaled answers purpose is to find the end user or engineer's mood about specific aspects of security classified projects. Interview results are almost self-explanatory, so these are not analysed separately.

5.1 Questionnaire analysis and possible solutions

In this chapter, the author reports the results in question order. In free-text responses, similar answers are calculated and treated as the same. Some of the free-text answers were very long and

included many different points. These are separated into smaller parts and joined together with similar responses. After every question, there are author recommendations based on the answers and analysis.

Question 1. Have you done security classified projects? responses

First was a filtering question to verify participants' involvement in security classified projects. Only one participant did not participate in security classified projects. All answers from this person were filtered out. There are a total of 32 valid responses. It happened because of some sort of filtering error on the raw data when filtering people who will get the questionnaire. The amount of valid responses is good for getting answers to research questions. In addition, it is high enough to get multiple challenges raised in free-text questions.

Question 2. Networks (On a scale of 1-5) responses

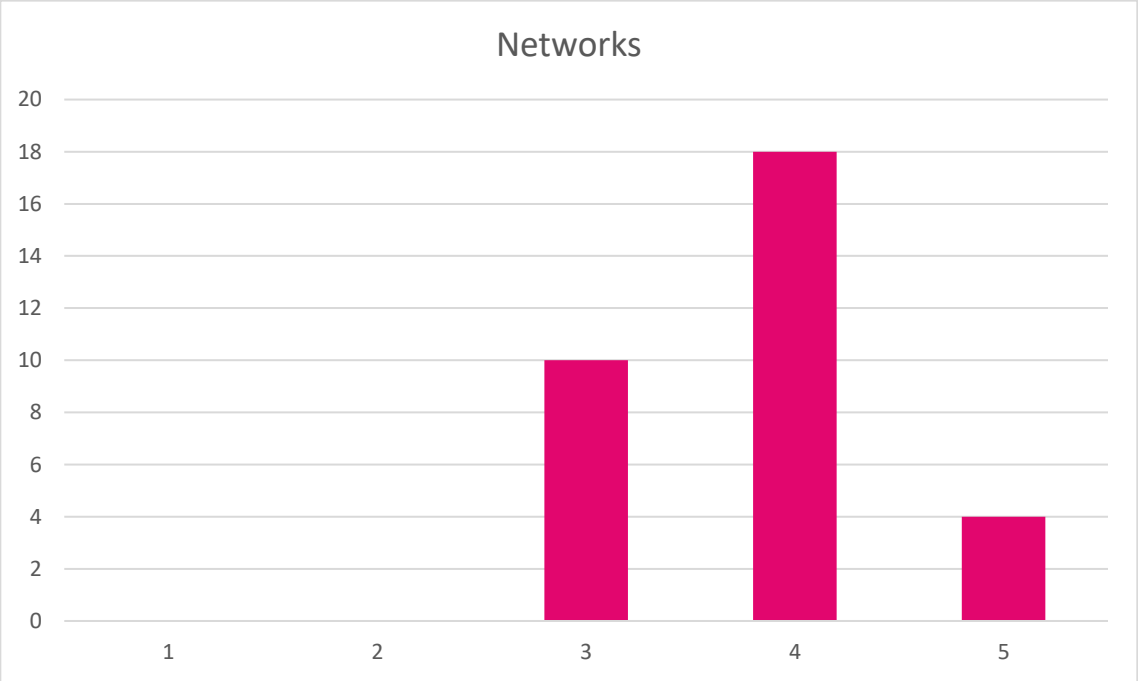


Figure 1: Question 2. Networks (On a scale of 1-5) responses

The question is about determining the mood of participants towards network functionality in secure classified projects. The average of the answers is 3.81. The lowest answer is three. Three is

ok, and four is good on this scale. Answers are closer to good than ok. It means that participants feel that the network functions well. This question would benefit from separating different security classifications since networks are not allowed in higher security classifications like TL III. There are different solutions for networking depending on the project. It means answers mean TL IV projects or lower classifications. Furthermore, it means network solutions work as intended on these projects, and there are no urgent issues with networks.

Question 3. Software (On a scale of 1-5) responses

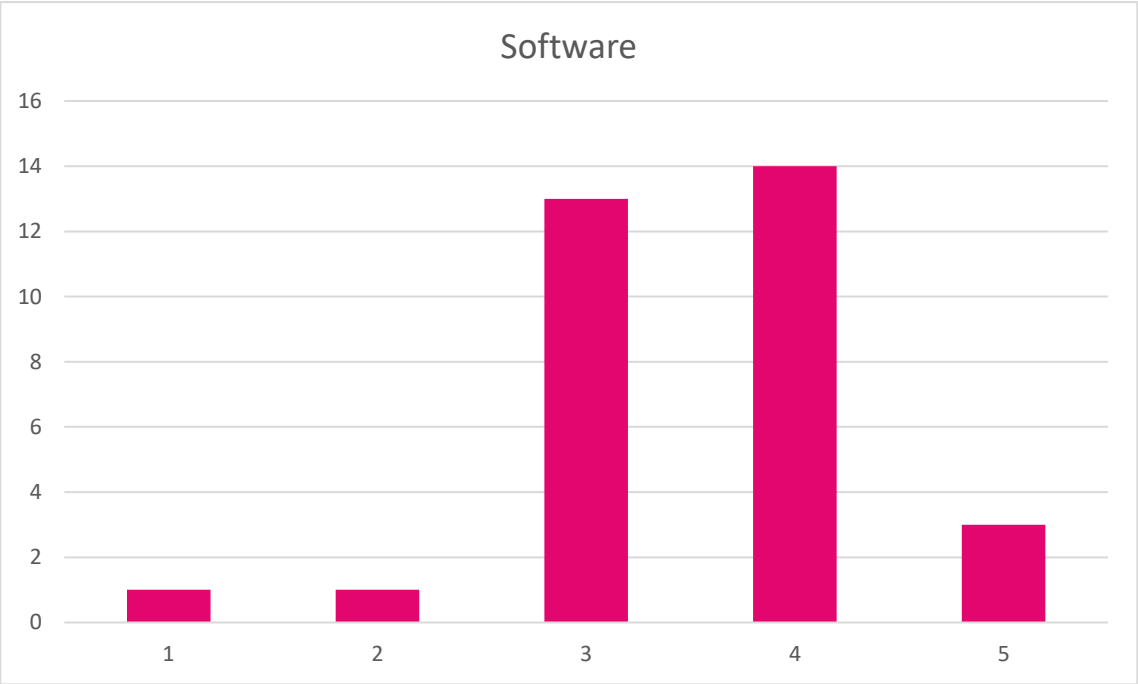


Figure 2: Question 3. Software (On a scale of 1-5) responses

This question determines how users feel about the software's functionality in security classified projects. The average of the answers is 3.53. The lowest answer is one, and the highest is five. Based on the average, which is between ok and good. Most designers do think that the software's functionality is adequate or reasonable. There were two unhappy designers, but the average was closer to good. The end user thinks the software functions acceptably in security classified projects. The result means the mood is almost good. Furthermore, licensing and other software issues affect end users less than IT management. IT management is trying to get everything working before users receive the device and start working on the security classified project. Based on the

results and the author's own experiences, pressure about software and licensing is in IT management.

Question 4. Computers (On a scale of 1-5) responses

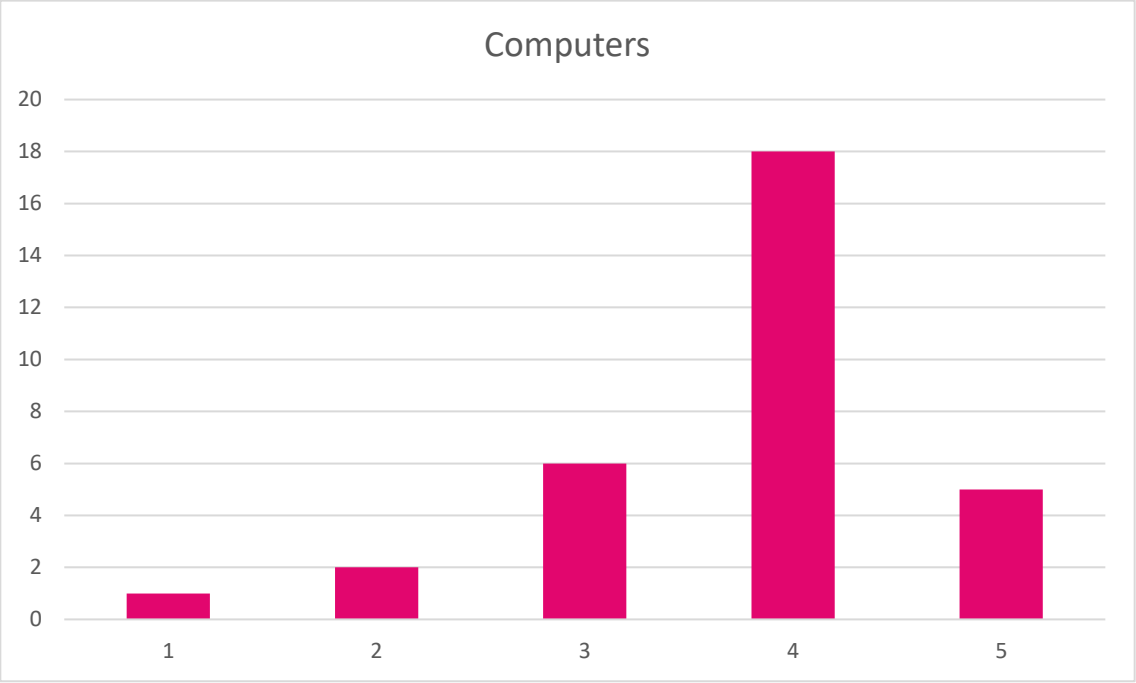


Figure 3: Question 4. Computers (On a scale of 1-5) responses

The average of the answers is 3.75. There is some broadness in results, but most designers think computers in security classified projects work well. Only one user answered one, which means really bad. Two users answered two, which means bad. The result is good from an IT management viewpoint. The result is reasonable because IT management tries to get everything working before giving the laptops to the user. Furthermore, it also means driver updates and other maintenance duties are done orderly.

Question 5. The flow of work (On a scale of 1-5) responses

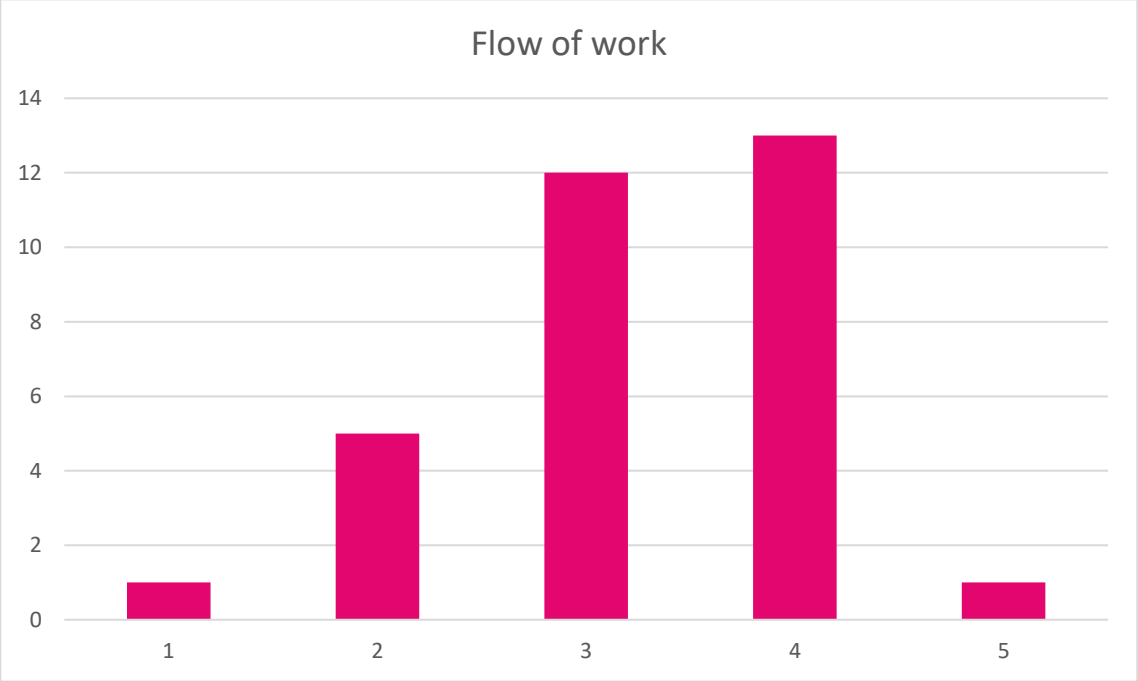


Figure 4: Question 5. The flow of work (On a scale of 1-5) responses

This question determines how users feel about the flow of work in security classified projects. The average of the answers is 3.25. However, the results are slightly over 3, which is only acceptable. It could be a better result. There are things to improve for the user experience and the flow of work.

Question 6. What kind of challenges have you encountered in classified projects?

Results are sorted in order by the highest number of similar responses. Six people answered that they had not experienced any issues and that everything had worked as it should.

Eight persons reported issues with communication and sharing data. Communication in security classified projects with colleagues is complicated when working in different physical offices. Because using emails and Teams is not allowed or possible. Also, missing network drive access makes sharing data difficult. Moving data between users and secured laptops with encrypted USB memory takes much work and time. In addition, customers' data classifications sometimes are very unclear and need clarification, causing problems with data handling.

Seven persons have experienced issues with instructions. Often instructions and restrictions received from customers could be more precise. In addition, customers often send instructions in multiple separate emails, which causes problems reading and understanding those instructions.

Six persons reported issues with design software. For example, design software needs an internet connection for licensing or a link to a database. Therefore, it is an issue when a customer demands work done in specific software which does not work without an internet connection. These six also reported issues with upgrading software or operating systems in secured laptops because of a lack of internet connection.

Five designers reported that more work resources need to have the necessary security clearance. Everyone working with security classified projects needs a security clearance. There need to be more designers with correct security clearance if there are holidays or sick leaves. The issue also affects IT management. Getting security clearance from the officials takes time. Company X cannot speed the officials, but it may proactively acquire authorisations for more designers.

Four designers experienced working with security classified projects much slower than regular projects. There are much more things to consider in security classified projects. Working in a secure room without the internet is more time-consuming nowadays. Moving data models with encrypted USB memory to secure laptop is much slower than downloading directly. Working is much slower with all requirements.

Three persons have had issues with encryption software. It takes time to learn to use all of them. There are multiple different kinds of encryption programs used in various states of secure projects. Sometimes customers demand to use a specific one. There are encryption methods for emails, data, USB memory and laptop.

Two designers feel that sometimes other companies do not share security classified data at all or data is incorrect. Asking for data again from partner companies is slow because of security classifications, which causes problems with actual design work and slows the work.

Two persons answered that remote working is not possible. It is an issue when there is a pandemic outbreak, flu season or just repairs in the office. Employees cannot work from home since networks are not allowed on secure laptops. There are some rare special occasions where the customer has allowed it when security can be proven, like, for example, covid-19 situation.

Customers' requirements are often tight. Not every data in the project is security classified. There are often public data that have security clearance. Then there are cases where involved partner companies do not share classified security data. Both cases cause issues with actual design work and also issues with the data classifications.

It is a challenge to remember all the different security requirements. These change with every customer and every project. There are many interpretations of the requirements.

Software installations to secure laptops sometimes cause issues. It takes time, especially if the location does not have IT personnel or IT personnel with security clearance since the software cannot be installed remotely because of a lack of network connectivity.

An issue reported by one user that it might be possible to accidentally users to leave old project data on secure laptops. In addition, sometimes programs leave temporary and cache files on temporary locations. The designer and IT management should ensure all project data is removed from the secure laptop.

Sending a secure email is challenging. Every customer has their practices and systems, and they keep updating or changing those. Sometimes ways and software for sending secure email change, and learning takes time.

Question 7. How large would you estimate the IT costs of a security classified project compared to a regular project? (On a scale of 1-5) responses

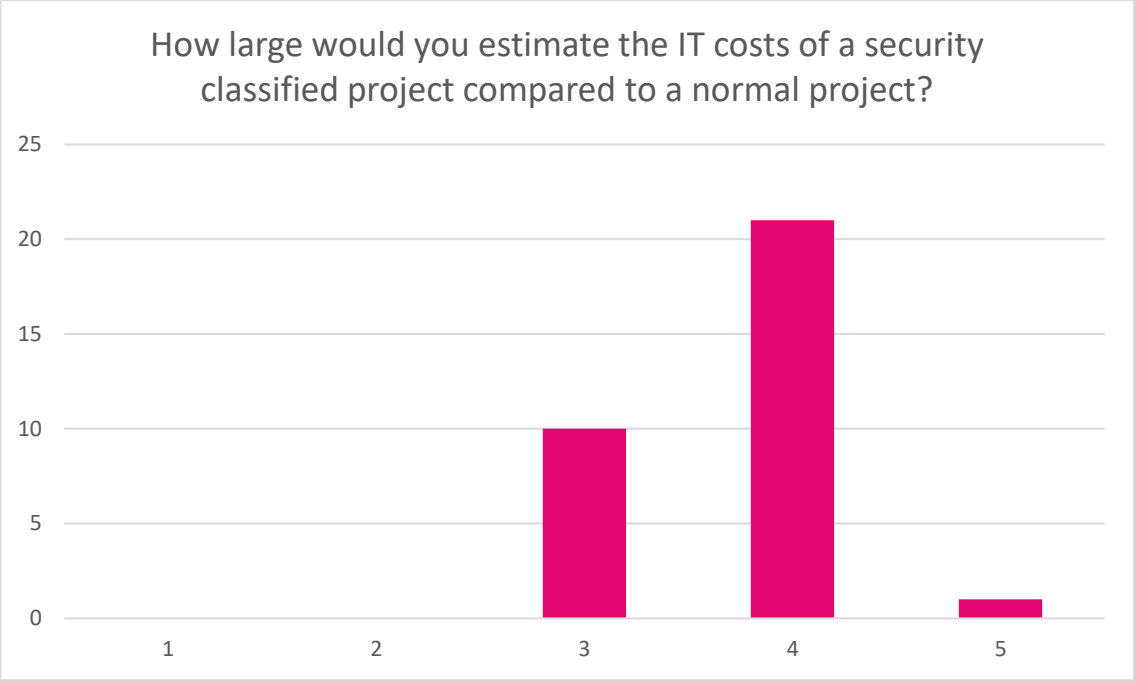


Figure 5: Question 7. How large would you estimate the IT costs of a security classified project compared to a regular project? (On a scale of 1-5) responses

The question tries to determine how the designers feel about the cost of a security classified project compared to a regular project. The average of the answers is 3.72. However, ten designers think the price is similar to a regular project. That is almost 1/3 of the responses. It confirms what we have suspected in IT management. Some users need to understand how costly security classified projects are. Because of this, offer prices for security classified projects might need to be higher, and some projects may need to be more profitable. Chapter 7 will have a more profound analysis of the costs.

Question 8. How would you evaluate the use of working time in a security classified project compared to a typical project? (On a scale of 1-5) responses

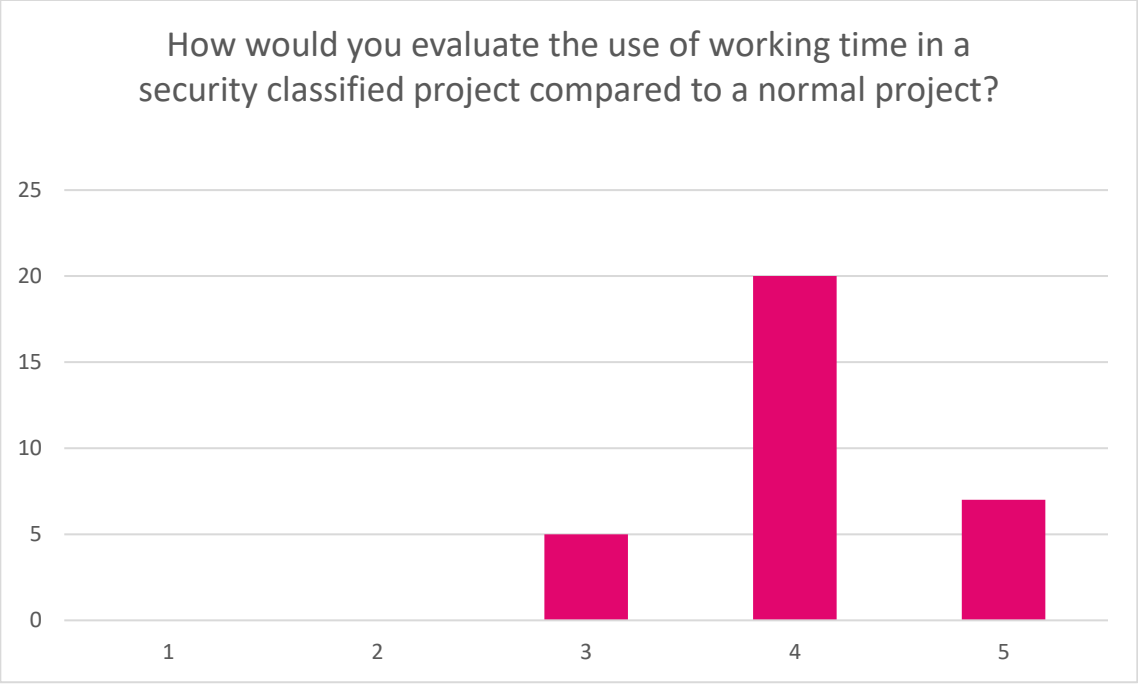


Figure 6: Question 8. How would you evaluate the use of working time in a security classified project compared to a regular project? (On a scale of 1-5) responses

The question tries to determine how the designers feel about working time in security classified projects compared to regular projects. The average of the answers is 4.06. Five designers feel that working time is similar on both projects. However, most designers think that security classified projects consume more working time. It was the expected result. IT management has noticed that these security classified projects are more time-consuming than regular projects. When comparing question 7 and question 8, it is clear that some designers do not consider their working time a cost. It will be analysed more in chapter 7.

Question 9. Do you feel the instructions and regulations are clear in security classified projects? (On a scale of 1-5) responses

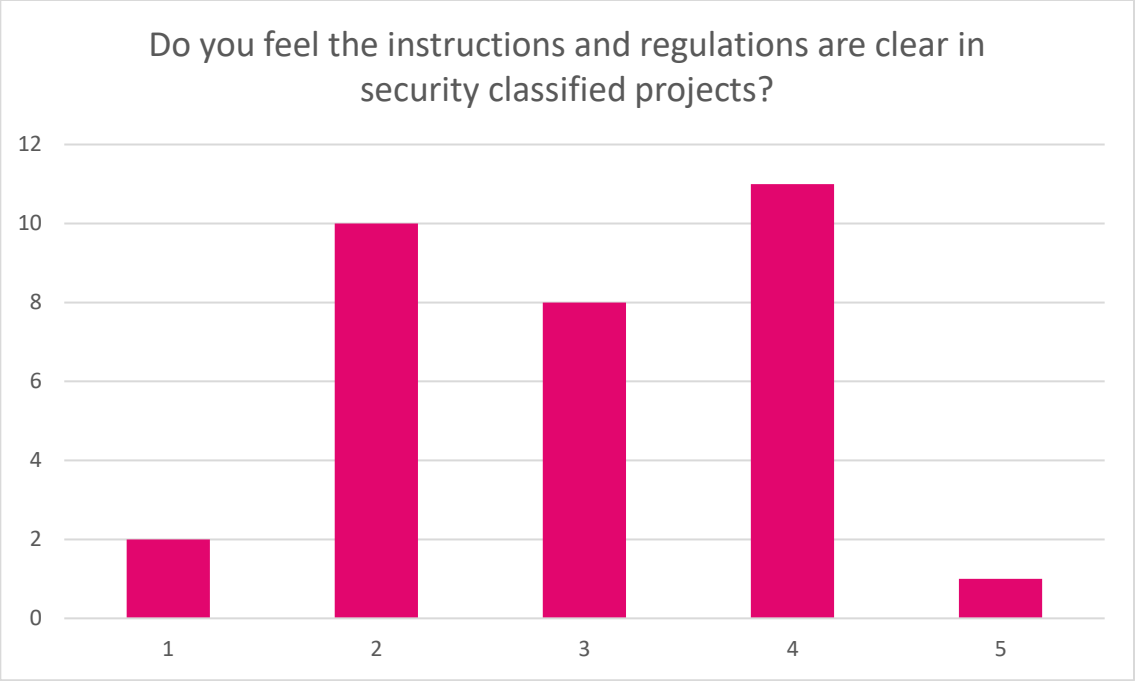


Figure 7: Question 9. Do you feel the instructions and regulations are clear in security classified projects? (On a scale of 1-5) responses

The question tries to determine how the designers feel about the clearness of instructions and regulations on security classified projects. The average of the answers is 2.97. There are some mixed signals here. Some feel instructions are clear (4) or very clear (5), and many people think the exact opposite. It might be because all security classifications were handled in the same question.

Question 10. How do you think the instructions could be improved? responses

There is much variation in answers. Some designers feel that instructions are self-explanatory and easy to understand, and some say the exact opposite. Ten people say that customers' instructions about security classified projects often need to be clarified. The exact amount of people said that customers' requirements and instructions vary with every project. These are a problem that Company X cannot fix alone.

Eight people answered that Company X's instructions were clear and reasonable. It is a much better result than expected. However, all the results indicate that much more work must be done, especially regarding processes and communication.

There are some excellent improvement ideas in the answers. For example, five people suggested instruction and regulation interviews with the customer when starting a new security classified project. It would help to clear requirements and give clear instructions on how the security classified project should be done. Two persons suggest better communication with the customer to combine instructions and methods of working. Also, when starting the new security classified project created internally, users approved of the project should get instructions and regulations automatically.

Five people feel that more education for Company X personnel working with security classified projects is needed. It is important. Instructions without educating them might be challenging to follow. Also, three persons feel that Company X internal instructions need improving.

Five people feel that some customers need help understanding what security classification means regarding costs—often demanding more secure classification even when it is not required. For example, projects starting data might already be public. Classification of public data to secure data does not secure it.

Four persons feel that instructions are difficult to find and suggested a centralised location. Sometimes customers send instructions in multiple emails, and sometimes message thread is difficult to follow. This email thread can be very long, and the risk of sharing security classified information accidentally rises. A centralised location would make instruction easier to access and comprehend.

There were some answers only suggested by only single person. For example, projects often have unrealistic time-table, which only allows designers to learn things while doing the work. Also, help is needed to remember all customer security requirements because they keep changing.

6 Possible solutions to identified challenges

At this point, the author has identified the ten most significant challenges in security classified projects, which are reported in table 1. Then, in this chapter, the author suggests possible solutions to those challenges. These solutions are based on answers in the questionnaire, interviews, and authors' views. In table 1 “persons reported” column is calculated by summarising results from interviews and questionnaire questions six and ten. Similar answers from different respondents are calculated as one. Based on table 1 author gets a criticality score for the challenge, and that order sorts the table.

Table 1: Identified challenges in order of persons reported.

Number	Challenge identified	Persons reported
1	Instructions and education	11
2	Software and licensing issues	10
3	Communication and sharing data	8
4	Costs of security classified projects	8
5	Workflow is much slower in security classified projects	7
6	Security clearance issues	5
7	Customer requirements and data classification issues	5
8	Encryption software issues and secure email issues	5
9	Remote working is not possible	3
10	Getting security classified data from partners	2

Challenge number 1: Instructions and education

Almost one-third of the people answering the questionnaire or interviewed say there is a need for improving instructions and guides. However, there were even good points about improving those. One of the most recommended is instruction and regulation interviews with the customer when starting a new security classified project. It should help understand why the security classified project is classified and help both parties understand instructions and reasons for regulations. Instructions and methods of working should be agreed upon together with the customer. Also, the instructions should be combined so that there is only one set of instructions for the designer or

engineer. The author agrees with this and recommends that this is a mandatory part of the project startup meeting.

The author also recommends that when a new worker is approved for the project, they get instructions automatically. Sharing instructions could be done using a centralised location for security classified project instructions. A centralised location would improve the quality of instructions, and the designer's workflow would improve. In addition, Worktime could be saved because there would not be a need to combine the instructions from multiple email threads. This approach also makes understanding the regulations of different security classified projects easier for designers. Regulations for security classified projects are very complex and manifold. There might be a way of instructions and regulations more straightforward. Straightforward and more uncomplicated instructions might help workers to understand them better.

Challenge number 2: Softwares and licensing issues

From an IT management viewpoint, this is a fundamental challenge. Because the need for network connectivity drives the ICT industry forward, and everything is connected. Every software and device needs connectivity. Since higher security classifications like TL III do not allow network connectivity using devices and software on those security classified projects is very difficult. Not having a network is a complex issue; no single solution can fix it.

For example, Autodesk and Microsoft products require network licensing. Autodesk does support offline licenses when using local network licenses. The only problem with these is the price. They are more expensive than regular network licenses. Microsoft Office, a simple everyday program used for documentation, no longer works with offline licenses. It requires a network connection every 30 days. The only way is to use some other program to do documentation (Microsoft Office 365,2023).

Then there are software updates and other issues with missing network connectivity. Even the Microsoft Windows operating system is slowly becoming an operating system that requires the network to install, operate, and license. This might cause issues in security classified projects (Microsoft Windows 11,2023).

The only viable solution is that customers allow limited network access to the vendor's licensing and updating servers. One solution might be a secure network without internet connectivity and a hosting server for licensing and updating. However, the solution would need, of course, to be audited and approved by authorities. There are network solutions that are security audited available, for example, SSH's NQX. This type of VPN solution with really advanced cryptology is used to connect different secure rooms. Connecting rooms would also help with challenge three: communication and sharing data. Since this might not be possible, the only way to handle this problem is to keep open communication with software vendors and have them keep supporting offline usage.

The author recommends calculating extra work hours for IT management and IT support. So that secured devices can be held up to date. Since updating and licensing will be manual work until network connectivity is allowed.

Challenge number 3: Communication and sharing data

The answers show that communication and data sharing is one of the most significant challenges. This issue can be tied to the same root problem as many other issues, the lost network connection. People have gotten used that everything is open and public as possible. Everyone can work anywhere using cloud services and instant chat messages. Secure email and phone calls are the only way to communicate with a security classified project colleague. In regular projects, there are file shares to share files between different locations instantly. People who have never used memory sticks come to work and must understand that it is the only way to share data in security classified projects. Using memory sticks also causes problems when working in different physical offices since they need to be transferred physically between offices. Using encrypted memory sticks is very time-consuming with different encryption software. This needs to be improved with workflows and ways of working.

The author recommends more education on memory sticks and encryption programs to people working on security classified projects. If this type of education is made a permanent part of security classified projects startup meetings, it will speed up communication and file sharing between partners and colleagues. This would save work time and smoothen the workflow. Connecting

secure rooms with VPN solutions that have been audited to TL III would also help to deal with this issue.

Challenge number 4: Costs of security classified projects

Costs of security classified projects did come up four times and indirectly multiple more times. Costs are crucial since IT management tries to keep costs down, but unique regulations for security classified projects make the costs higher than regular projects. Based on interviews, costs are typically two to seven times higher than in regular projects. The author will analyse the cost in more detail in chapter 7.

Challenge number 5: Workflow is much slower in security classified projects

Working with a security classified project is much slower than in a regular project. As accomplished with questionnaires and interviews, working in a secure room is slower than in a standard office, and communication and file-sharing are slower than in regular projects. Using memory sticks and encryption programs takes time, especially in higher security classified projects. Comprehending all the requirements also takes work time. The author thinks that streamlining instructions and helping designers to understand the regulations will make security classified projects more efficient.

The author suggests making instruction and regulation interviews an integral part of project startup meetings to make this more efficient. Security classified projects will always be slower than regular projects because of an entirely different workflow, but people can learn that with education and instructions.

Challenge number 6: Security clearance issues

Five persons feel that there is an issue with having too few personnel with security clearances for security classified projects. A security clearance is not precisely an IT management issue but also affects IT management and IT support personnel. Supporting security classified devices might be problematic if there are too few personnel with necessary clearances when there are sick leaves

or vacations. Getting security clearances for officials takes much time, and support is often needed immediately. This should be taken into consideration early.

The author recommends that Company X proactively acquire enough authorisations for security-cleared personnel to make and support security classified projects.

Challenge number 7: Customer requirements and data classification issues

Five persons reported that there had been issues with classification, especially on the customer's side. It is not an IT management issue but will affect workflow and costs. Sometimes classifications change in the middle of the project. Data has been classified wrongly—for example. Public data is classified as TL III. There have even been cases where that project started as a security classified and changed to a regular project midway. All these issues cause problems in workflow and spending working time. They can also affect data security if the classification is wrong.

The author recommends discussing this classification issue with a customer in a project startup meeting. It should be made a permanent article for the first meeting. Classifications come from customers, and the only thing Company X can do is open communication with the customers. Open communication with the issue and making it part of project meetings might help.

Challenge number 8: Encryption software issues and secure email issues

Five persons reported that sending secure emails is challenging. There are customer-related secure email solutions that often work differently than regular email. Learning these systems takes work time. For example, sometimes customers demand to use of a specific encryption program used to encrypt USB memory sticks. Since multiple programs are available, the engineer or designer is only used to using some of them.

The author recommends more education for engineers and designers. In addition, secure email systems and encryption software should be integral to project management and instructions. When it is an integral part, it will raise security awareness and make working more secure.

Challenge number 9: Remote working is not possible

Some engineers and designers feel that remote working should be allowed in security classified projects. In comparison, in recent incidents like COVID-19, people have learned to take remote work as part of the workflow. Keeping the data secure when working at home or coffee shop is difficult. Those places cannot be trusted. Someone can see something classified as data or steal the laptop. The author understands this wish from the end user's viewpoint, but keeping the data safe outside a physically secure location would be impossible. Katakri subdivision physical security (F) prohibits this (Ulkoministeriö, 2021c).

Challenge number 10: Getting security classified data from partners

Getting security classified data from partners is not an IT management challenge itself. However, the issue was mentioned in a few answers, and it seems that when third-party contractors are involved, there are data-sharing issues in security classified projects. Sometimes third parties do not share classified data, or the data itself needs to be more detailed. Using USB memory sticks and secure email for sharing data is slow and complex. These are similar issues handled in challenges one (Instructions and education), three (Communication and sharing data), seven (Security clearance issues) and eight (Encryption software issues and secure email issues).

The author recommends opening communication with all involved parties in security classified project startup meetings. In the end, this is an issue that the customer should fix.

7 Analysis of IT costs in security classified projects

Based on the interview and questionnaire, IT costs of security classified projects are much higher than regular projects. In this chapter, the author tries to find a multiplier to help better understand the costs. Multiplier is a simple way of telling how much more security classified project costs are compared to a regular project. This part of the research is not exact since many factors affect these costs. That is the reason for choosing a multiplier and not a euro amount. These costs

can, of course, go higher and lower based on economic changes. The purpose is to make a table that can estimate costs. The user of this table needs to know the IT costs. Some details are vague to protect Company X and the partners. For example, office or secure room costs are not taken into consideration. The background of the table is explained in the following sections.

Base costs. Device price and installation of security classified laptop

In security classified projects, the device costs the same as used in a regular project. However, designer or engineer IT costs are double since they have also devices used in regular projects. Both devices need displays, keyboards, mouses and other peripheral devices. In security classified projects, there are separate devices and separate licenses—a total multiplier of 2x.

Installing a regular desktop or laptop PC in an entirely usable state takes about 1,5 hours. Installation here means an operating system with all possible updates and all the software user needs to do the work. Time is dependent on which software is needed by the end user. Installation is fully automated. In devices used in security classified projects, there is no automation involved. Installation takes about 5 hours in total. This means a multiplier of 3,33x.

Updates and maintenance of security classified laptop

In devices used in regular projects, updates are automated. This means there are no extra work hours needed. Devices used in security classified projects updating and maintenance work is manual work. IT support needs to do everything manually and in location. This also means travelling time. The author estimates that travelling time is usually two hours in one-way depending on the office location. Usually, updating OS and software and doing maintenance work takes about four hours. Calculating travel time and work time together means eight hours of work time. This cost depends on how often update cycles are done. The author calculates one-month, three-month and six-month cycles in the table. This value can be more accurate by measuring the time spent on the updating cycle and travelling time. Here the author uses a rough estimate—a multiplier of 8x per update cycle.

Software licences for security classified laptop

Software licensing costs are double at a minimum. Because the designer or engineer already has licenses on a regular device. Security classified device software licenses are almost all one-year offline licenses with a fixed one-time price. Because of this, the usage time of security classified devices should be high to keep the costs down per project. However, keeping usage high might be difficult because of the nature of security classified projects. The author has calculated the multiplier with three percentages 50%, 25% and 10%. 50% usage time means the device is used for 50% of workdays. In the year 2023, there are 226 workdays. (Teknologiateollisuus, 2022)

Table 2: Regular project vs security classified project cost multipliers

	Multiplier	**Type**			
Base costs					
Device price	2	Price			
Installation	3,33	work hour			
Maintenance cycles			**one-month**	**three-month**	**six-month**
Updates and maintenance	8	work hour	96	32	16
Software usage time percentage			**50 %**	**25 %**	**10 %**
Software licenses	1	Price	0,5	0,75	0,9

Table 3 presents example for calculating costs using the multipliers. In this example, prices are made up by the author and not based on anything real. The device costs 2500€. IT support work hour costs 65€ and the software license 10000€/year.

Table 3: Example calculation using multipliers

	Multiplier				
Base costs		**€**	**Total**		
Device price	2	2500	5000		
Installation	3,33	50	166,5		
Maintenance cycles			**one-month**	**three-month**	**six-month**
Updates and maintenance	8	work hour	96	32	16
Work hour cost / €	50		4800	1600	800
Software usage time percentage			**50 %**	**25 %**	**10 %**
Software licenses	1	Price	0,5	0,75	0,9
License cost /€ per year	10000		5000	7500	9000

Using table 3 For example, we can use a six-month maintenance cycle and a 10% usage percentage to get the total IT costs. Base costs: 5000€+166,50€=5166,50€. Update and maintenance costs per year 800€. The license cost per year is 9000€—total costs of 14966,50€ for the first year. Next year 9800€/year.

In a regular project, similar costs would be device costs and license costs from the 50% column because licensed software would be in use more. So costs would be 2500€+5000€ for the first year—next year 5000€. The highest single cost is software licenses, and there is a clear cost difference even with made-up numbers from costs. Based on these numbers, total security classified project IT costs are double. These numbers only have some of the work hours included. Many small meetings, phone calls and planning are not included.

8 Conclusion

The research was successful and did find lots of challenges and issues. The author identified possible challenges at the beginning of the research. These identified challenges were very different from those the engineers and designers reported. Only three of the challenged identified by the author were reported by the respondents. There is an issue with licenses, updates and remote

connections because of a missing internet connection. There is need for security clearances for IT personnel and high costs of security classified projects. The author was thinking of issues very narrow-minded. The top ten issue lists are broader than the challenges identified by the author at the beginning of the research. It is valuable information regarding how different people working in IT management think compared to end users. The author thinks this research is excellent and helpful for broadening the thinking of IT management people. Sometimes IT management is alone in an ivory tower, and issues seem narrower and more technical than they are.

Doing the research was very interesting. The author regrets not separating classes of different security classified projects in the questionnaire. Overall, that only affected the data a little. The author learned a lot from this research and how to think about security classified projects from different perspectives. This research has broadened the author's mind from technical to people issues. The author sees this as a good thing. Cyber security is a people issue, not a technical issue. It is about the way of thinking, the way of doing things and understanding why.

This research shows that the biggest issue is instructions and education. That is not a technical issue. It is an issue that can be solved by understanding the designer's and engineer's workflow. The author recommends that project startup meetings include instructions, guides and regulations as an integral part. Then the knowledge of how to work in security classified projects rises, and there would be less confusion. It would also help the customer understand which data need to be classified and why security classified projects cost more. The author thinks this crucial change in the work method would help to make security classified projects more efficient and workflow smoother. The change would also improve communication with the customer and engineers.

One change can not fix everything. There are many challenges in security classified projects. New network solutions may be helpful in security classified projects. These new network solutions can link TL III rooms with a secure network. That would make things easier. IT support could give support remotely from the different secure rooms and one network licensing server to support all secure rooms. Those things might be the future. One thing is sure. Secure network solutions are needed for these secure classified projects. This research was only for one company, but the author hopes it will help others. Company X was happy with this research, which helped broaden the

whole concept of security classified projects. Talks after the questionnaire and interviews have boosted the development of these projects in IT management.

The world has changed a lot since the author started this study. There is a war in Europe, and cyber security is more important than ever, which means security classified projects are more important than ever. Finland has become member of a NATO. Keeping the sensitive data secret and safe is the most important thing nowadays.

References

Cambridge University Press. (2022). *Meaning of project in English.* Retrieved October 5, 2022, from https://dictionary.cambridge.org/dictionary/english/project

Gary Hibberd. (2022). *Art of Cyber Security - A practical guide to winning the war on cyber crime.* IT Governance Publishing. Retrieved November 3, 2022, from https://masterworkshop.skillport.com/skillportfe/main.action?assetid=162713

IBM. (2023). *What is IT management?* Retrieved January 16, 2023, from https://www.ibm.com/topics/it-management

JAMK. (2018). *Pedagogical and Ethical Principles.* Retrieved from Studyguide: https://studyguide.jamk.fi/en/study-guide-masters-degrees/information-about-jamk/pedagogical-and-ethical-principles

Kananen, J. (2015). Opinnäytetyön kirjoittajan opas – Näin kirjoitan opinnäytetyön tai pro gradu-nalusta loppuun. [Thesis Writer's Guide - This is how I write the thesis or pro gradu from the beginning to the end]. Jyväskylän ammattikorkeakoulu.

Microsoft Forms.(2022). *Microsoft Forms help & learning.* Microsoft. Retrieved November 7, 2022, from https://support.microsoft.com/en-GB/forms

Microsoft Office 365.(2023). *Overview of licensing and activation in Microsoft 365 Apps* Microsoft. Retrieved January 22, 2023, from https://learn.microsoft.com/en-us/deployoffice/overview-licensing-activation-microsoft-365-apps

Microsoft Windows 11.(2023). *Find Windows 11 specs, features, and computer requirements*. Microsoft. Retrieved January 22, 2023, from https://www.microsoft.com/en-us/windows/windows-11-specifications

Piiparinen, P. (2021). *Turvaluokitellun hankkeen erityispiirteet.* Retrieved from https://www.theseus.fi/handle/10024/501557

Portney, L. (2019). *Foundations of Clinical Research: Applications to Evidence-Based Practice.* 4th edition, F.A. Davis Company.

Schmidt, C. (2004). *The analysis of semi-structured interviews.* U. Flick, E. von Kardorff & I. Steinke. A Companion to Qualitative Research. London, Thousand Oaks, New Delhi: SAGE Publications, 253–258.

Tasala, K. (2020). *Projektipäällikkönä palvelinkeskuksen KaTaKri-luokitellussa laajennushankkeessa ja turvallisuustekniikan päivitysprojekteissa.* https://www.theseus.fi/handle/10024/352375

Teknologiateollisuus. (2022). *Teollisuuden työntekijöiden työaika 2022-2023.* Retrieved January 15,2023, from https://teknologiateollisuus.fi/sites/default/files/2022-01/Vuosity%C3%B6aika_2022-2023.pdf

Theseus. (2023). *Open Repository Theseus - the theses and publications of the Universities of Applied Sciences on the Internet.* Retrieved from https://www.theseus.fi/

Ulkoministeriö. (2021a). *Katakri – tietoturvallisuuden auditointityökalu viranomaisille*. Retrieved from https://um.fi/Katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

Ulkoministeriö. (2021b). *Information security auditing tool for authorities – Katakri*. Ministry for Foreign Affairs. Retrieved from https://um.fi/information-security-auditing-tool-for-authorities-Katakri

Ulkoministeriö. (2021c). *Katakri 2020 Information Security Audit Tool for Authorities.* Ministry for Foreign Affairs. Retrieved from https://um.fi/documents/35732/0/FINAL+-+Katakri-2020_201218_en.pdf

Vaarasalo, J. (2021).*TL IV luokiteltu monihankeympäristö.* Retrieved from https://www.theseus.fi/handle/10024/509676

VAHTI. (2023). *Vahti-ohjeet* Retrieved January 16, 2023, from https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet

Valtiovarainministeriö (2021). *Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä.* Ministry of Finance. Retrieved from https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162649/VM_2021_5.pdf

Appendices

Appendix 1. Questionaire questions from Microsoft Forms in Finnish

Tietoturvaluokiteltujen projektien haasteet IT:n näkökulmasta

Hei!

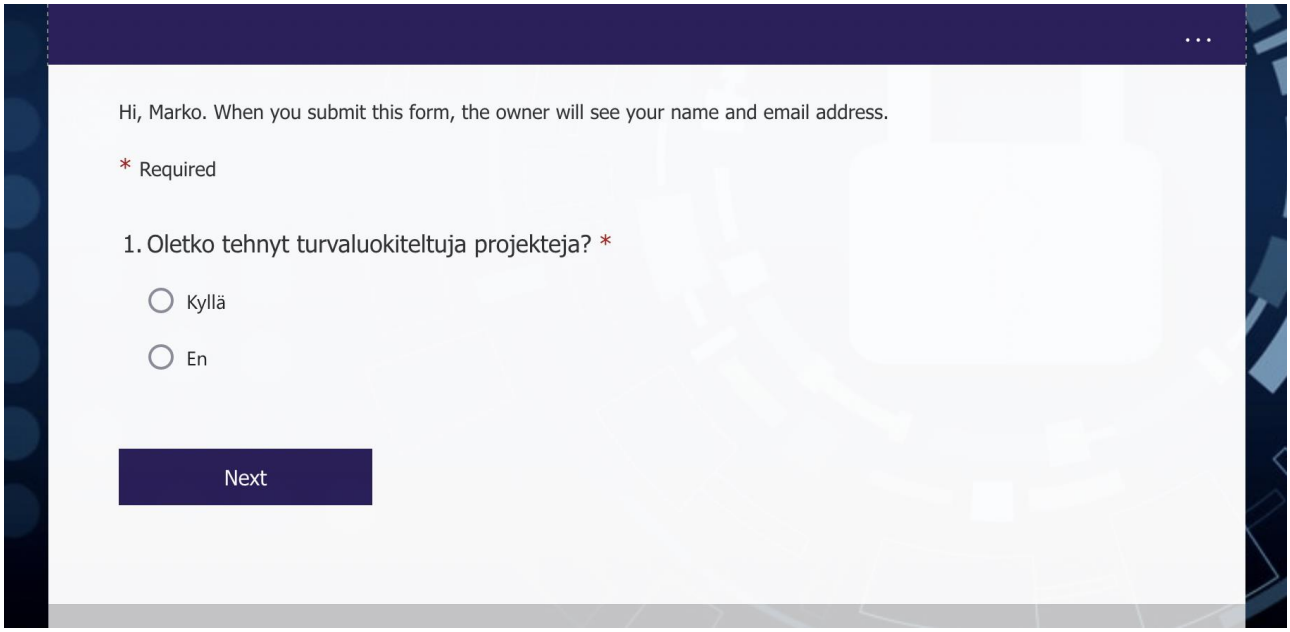
Opiskelen Jyväskylän ammattikorkeakoulussa Cyber Security -koulutusohjelmassa (YAMK).
Teen opiskeluihini liittyen opinnäytetyötä aiheesta "Security challenges of classified projects".
Tietoturvaluokiteltujen projektien haasteet IT:n näkökulmasta.

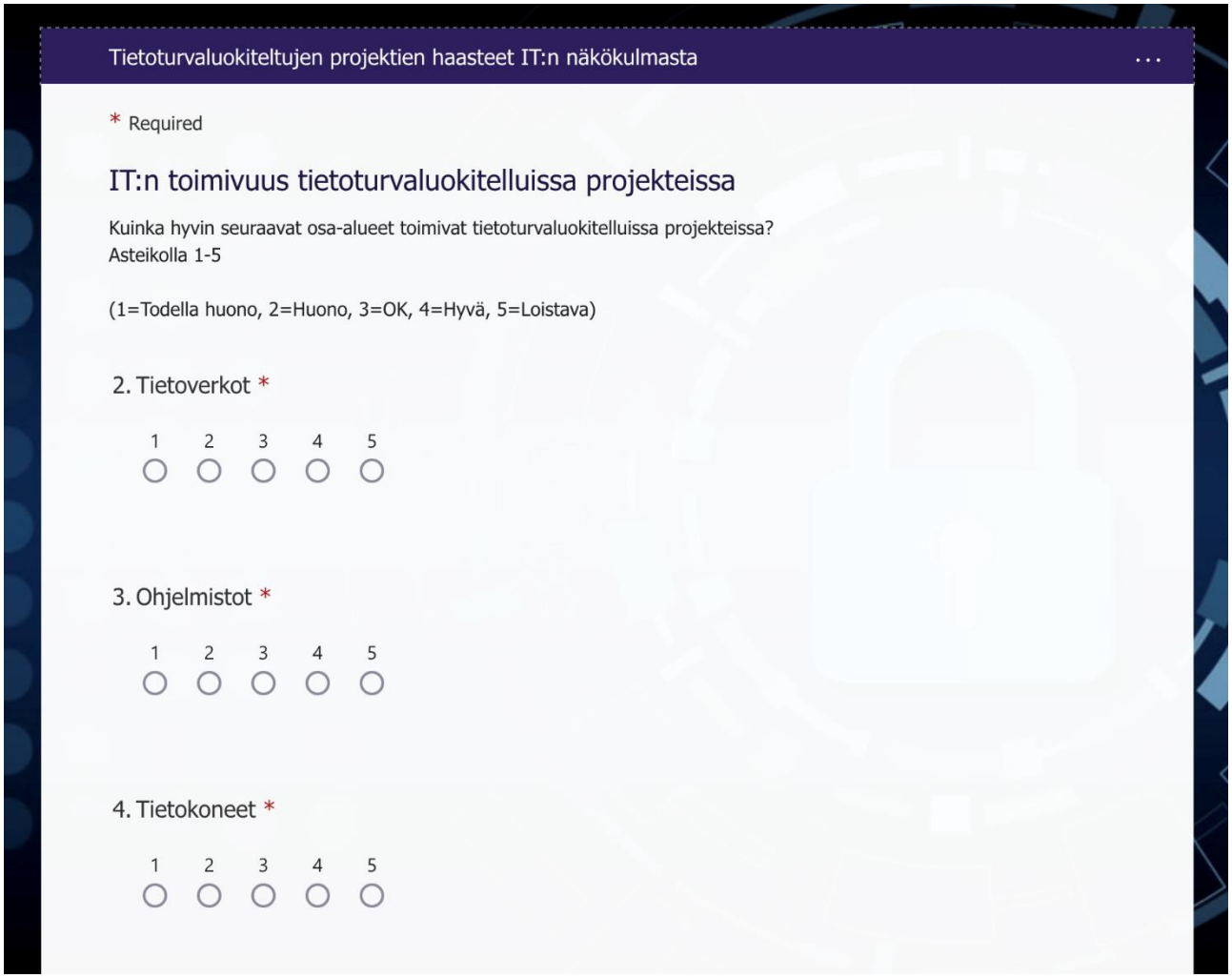
Tietoturvaluokitelluissa projekteissa on omanlaisensa haasteet IT:n näkökulmasta.
Tietoturvaluokitellut projektit tulevat myös varmasti lisääntymään jokaisella liiketoimintaalueella.
Siksi näiden haasteiden kartoittaminen on erittäin ajankohtaista.
Opinnäytetyöni tarkoitus on havaita mahdollisimman monia näistä haasteista, analysoida niitä ja mahdollisesti yrittää löytää ratkaisuja niihin.
Tämä työ pyrkii auttamaan projektien kustannusten hallinnassa ja tarjousten laadinnassa.
Työstä syntyvä lopputulos yrittää löytää tehokkaampia tapoja IT:n toimintamalleihin ja tuoda projektien IT-kustannukset lähemmäs oikeita kustannuksia.
Itse opinnäytetyö toteutetaan englanninkielellä, joten englanninkieliset vastaukset käyvät myös.

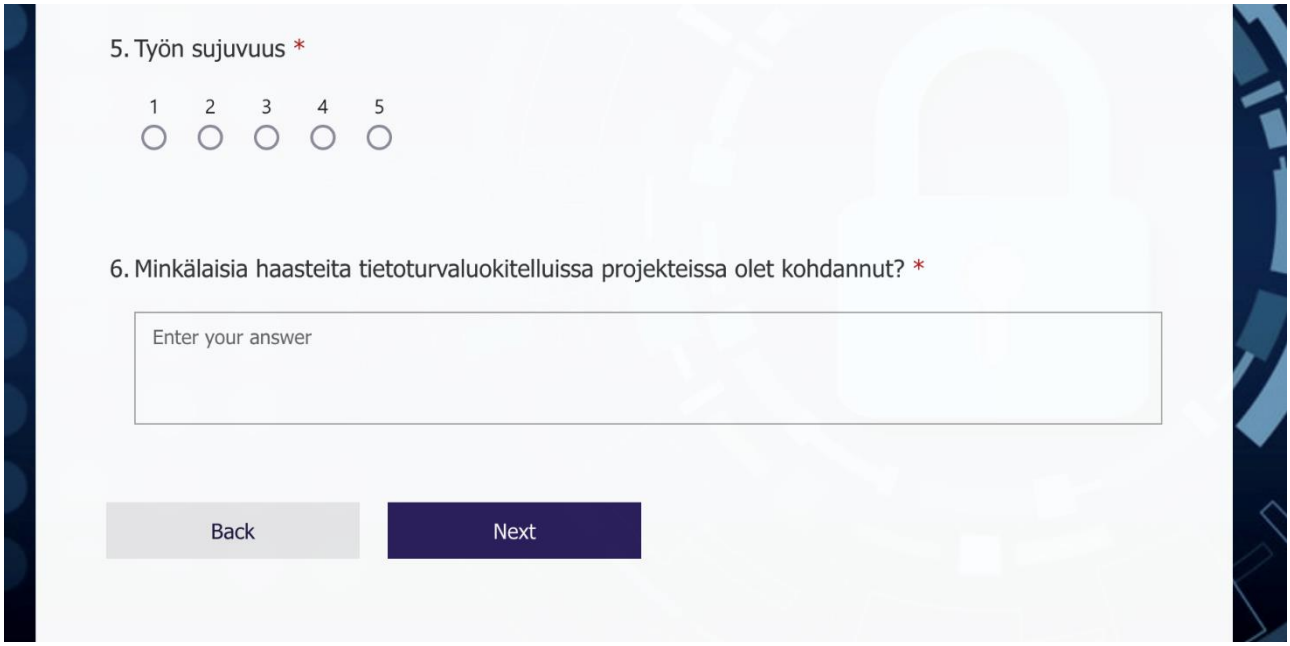
Kyselyyn vastaaminen:
Vastaaminen tapahtuu täyttämällä tämän kyselyn 01.10.2022 mennessä.
Vastaamiseen menee muutama minuutti.

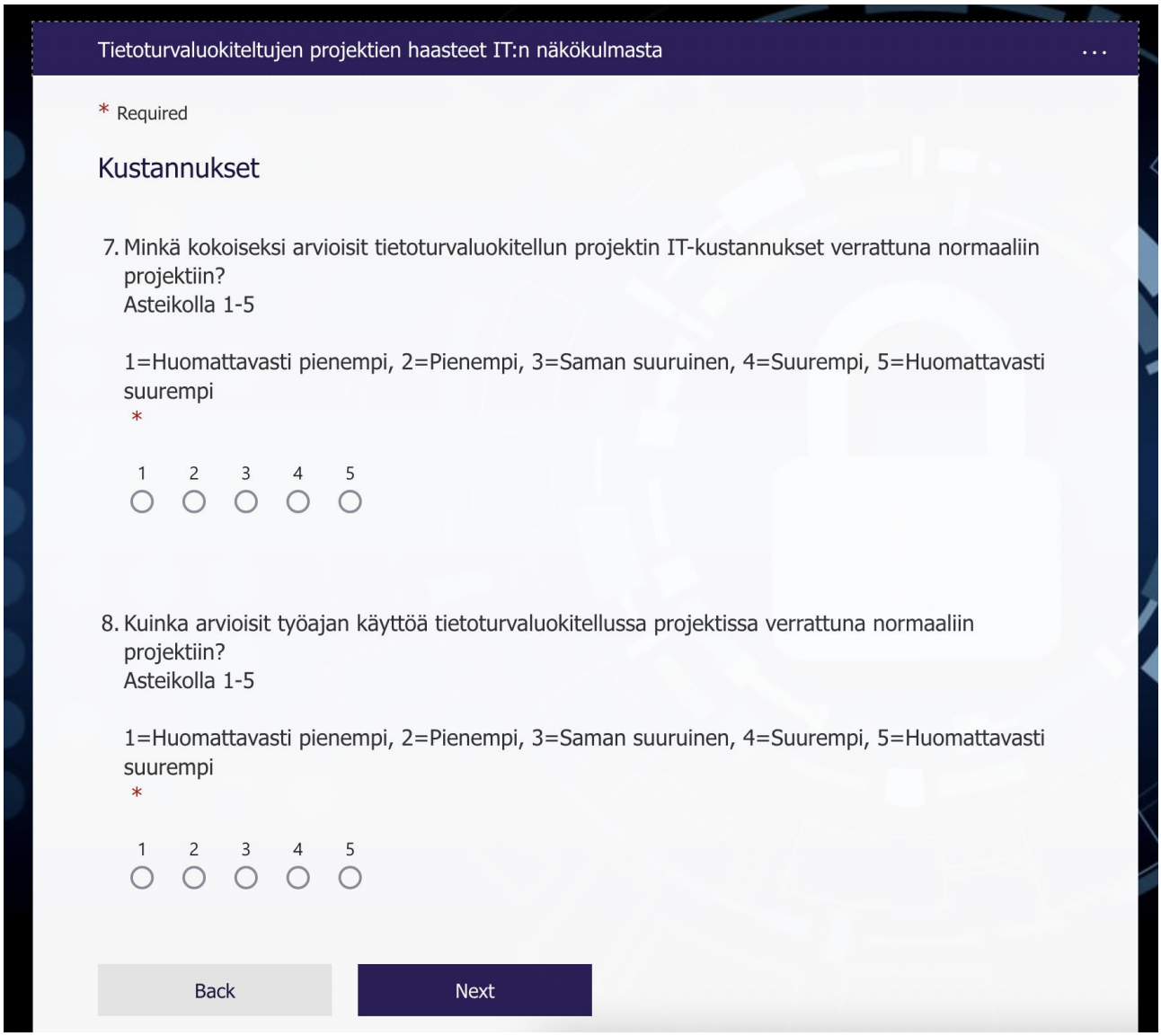
Vastaajien henkilöllisyys on vastausvaiheessa vain tutkijan tiedossa ja lopullisessa työssä vastaukset on raportoitu siten, että niistä ei voi tunnistaa henkilöitä, projekteja, liiketoimintaalueita, eikä järjestelmien nimiä. Tutkimuksessa syntynyttä ja/tai opiskelijalle luovutettua aineistoa käytetään vain tässä viestissä kuvatun tutkimuksen tekemiseen. Tutkimusaineiston keräämisessä, käsittelyssä, säilyttämisessä ja tuhoamisessa noudatetaan henkilötietolakia, sekä hyvää tutkimusetiikkaa. Kyselyyn osallistuminen perustuu vapaaehtoisuuteen.

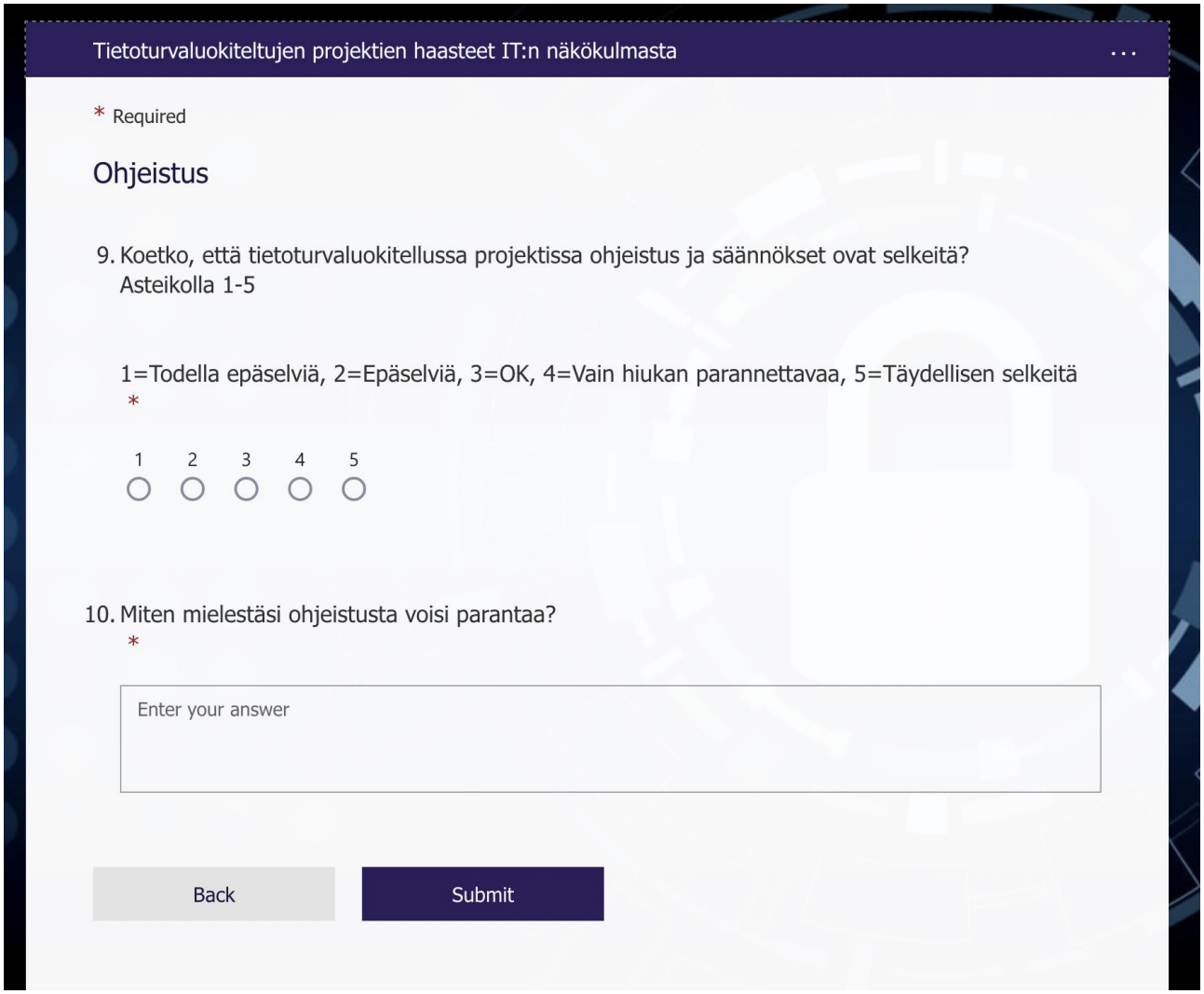
Kiittäen,
Marko Lehtinen


...
Hi, Marko. When you submit this form, the owner will see your name and email address.
* Required
1. Oletko tehnyt turvaluokiteltuja projekteja? *
Kyllä
En
Next


Tietoturvaluokiteltujen projektien haasteet IT:n näkökulmasta
...
* Required
IT:n toimivuus tietoturvaluokitelluissa projekteissa
Kuinka hyvin seuraavat osa-alueet toimivat tietoturvaluokitelluissa projekteissa?
Asteikolla 1-5
(1=Todella huono, 2=Huono, 3=OK, 4=Hyvä, 5=Loistava)
2. Tietoverkot *
1 2 3 4 5
3. Ohjelmistot *
1 2 3 4 5
4. Tietokoneet *
1 2 3 4 5


5. Työn sujuvuus *
1 2 3 4 5
6. Minkälaisia haasteita tietoturvaluokitelluissa projekteissa olet kohdannut? *
Enter your answer
Back
Next


Tietoturvaluokiteltujen projektien haasteet IT:n näkökulmasta
* Required
Kustannukset
7. Minkä kokoiseksi arvioisit tietoturvaluokitellun projektin IT-kustannukset verrattuna normaaliin projektiin?
Asteikolla 1-5
1=Huomattavasti pienempi, 2=Pienempi, 3=Saman suuruinen, 4=Suurempi, 5=Huomattavasti suurempi
*
1 2 3 4 5
8. Kuinka arvioisit työajan käyttöä tietoturvaluokitellussa projektissa verrattuna normaaliin projektiin?
Asteikolla 1-5
1=Huomattavasti pienempi, 2=Pienempi, 3=Saman suuruinen, 4=Suurempi, 5=Huomattavasti suurempi
*
1 2 3 4 5
Back
Next


Tietoturvaluokiteltujen projektien haasteet IT:n näkökulmasta
...
* Required
Ohjeistus
9. Koetko, että tietoturvaluokitellussa projektissa ohjeistus ja säännökset ovat selkeitä? Asteikolla 1-5
1=Todella epäselviä, 2=Epäselviä, 3=OK, 4=Vain hiukan parannettavaa, 5=Täydellisen selkeitä *
1 2 3 4 5
10. Miten mielestäsi ohjeistusta voisi parantaa? *
Enter your answer
Back
Submit