NTNU

Norwegian University of
Science and Technology

Recommendations for Improvement of Security Requirements in Norwegian Public Procurements

Hans Kristian Henriksen

Master of Science in Computer Science	
Submission date:	June 2016
Supervisor:	John Krogstie, IDI
Co-supervisor:	Lillian Røstad, ITEM

Norwegian University of Science and Technology
Department of Computer and Information Science

Abstract

Every year, the Norwegian government and its organisations acquire a large number of new IT-systems. These must be bought through a well regulated and rigid procurement process, where system requirements must be clearly formulated ahead of time. This is especially a challenge for security requirements, as changes to the system and the technological development might render such requirements outdated quickly.

This thesis investigates the security requirements of publicly procured IT-systems and how they are impacted by the procurement process.

In total, 14 participants were interviewed to provide insight into the three research questions: (1) How is the current state of security requirements in public procurements viewed by procurers and suppliers? (2) What challenges exists when procuring IT-systems, and how does this affect security requirements? (3) What recommendations can be given to improving the current state of security requirements in public procurements?

The participants reported insufficient security focus and competence both for procurers and suppliers, and generally inadequate security requirements. Security requirements were often given low priority by both procurers and suppliers. While the procurement process was viewed as a good tool to ensure fair competitions, security requirements were dropped or modified in order to ensure enough competition for bids, too few tenders were reported to be using negotiated processes, and the transparency demands were seen to impact security requirements especially.

The thesis provided four recommendations for improving the state of security requirements in Norwegian public procurements: (1) A negotiated process should be used when procuring IT-systems. (2) Standardised checklists for security requirements should be developed. (3) Security competence must be retained in procuring organisations, and (4) The security focus in the governmental standard terms and conditions (SSA) must be improved.

The main limitations of the study were the number of participants, and the fact that participants were recruited from the personal network of the author and advisors, and were thus not representative of the industry as a whole. Further recommended work includes an extended study with a random selection of participants, case studies of single procurements, and the development of the recommended checklists.

Sammendrag

Hvert år anskaffer norske offentlige organisasjoner et stort antall IT-systemer. Disse må kjøpes gjennom en velregulert og rigid anskaffelsesprosess, hvor systemkravene må være tydelig formulert på forhånd. Dette er en spesiell utfordring for sikkerhetskrav, siden endringer i systemet, og den teknologiske utviklingen hurtig kan føre til at disse kravene blir utdatert.

Denne oppgaven undersøker sikkerhetskravene i offentlig anskaffede IT-systemer, og hvordan disse påvirkes av anskaffelsesprosessen.

Totalt ble 14 deltakere intervjuet for gi innsikt i de tre forskningsspørsmålene: (1) Hvordan ser anbudsgivere og tilbydere på den nåværende tilstanden til sikkerhetskrav i norske offentlige anskaffelser? (2) Hvilke utfordringer er det når IT-systemer anskaffes, og hvordan påvirker disse sikkerhetskravene? (3) Hvilke anbefalinger kan gis for å bedre den nåværende tilstanden til sikkerhetskrav i offentlige anskaffelser?

Deltakerne rapporterte utilstrekkelig sikkerhetsfokus og kompetanse både hos anbudsgivere og tilbydere, og generelt for dårlige sikkerhetskrav. Sikkerhetskrav ble ofte gitt lav prioritet av både anbudsgivere og tilbydere. Selv om selve anbudsprosessen ble sett på som et godt verktøy for å sikre rettferdig konkurranse, blir sikkerhetskrav utelatt eller modifisert for å sikre nok konkurranse om anbudene, for få anbud bruker anskaffelsesprosesser med forhandlinger, og kravene til åpenhet påvirker sikkerhetskrav spesielt.

Oppgaven presenterte fire anbefalinger til forbedringer for sikkerhetskrav i offentlige anskaffelser: (1) En prosess med forhandlinger bør brukes når IT-systemer anskaffes. (2) Standardiserte sjekklister for sikkerhetskrav bør utvikles. (3) Sikkerhetskompetanse må beholdes i anskaffende organisasjoner, og (4) Sikkerhetsfokuset i Statens Standardavtaler (SSA) må forbedres.

Hovedbegrensningene i studien var antallet deltakere, og det faktum at deltakerne ble rekruttert fra det personlige nettverket til forfatteren og veilederne, og dermed ikke er representative for industrien som helhet. Videre anbefalt arbeid inkluderer en utvidet studie med et tilfeldig utvalg av deltakere, case-studie av enkeltanskaffelser, og utviklingen av de anbefalte sjekklistene.

Acknowledgements

Working on a thesis of this size, and a source material as extensive, has been a real challenge. Many cups of coffee and tea have been drunk, and a lot of midnight oil has been burned. But it is not only my own work that has been vital for the completion of this thesis.

Firstly I would like to thank Lillian Røstad. As my external advisor, she has been an invaluable source of information, provided me with access to her contacts, corrected me when I have misunderstood central concepts, and pushed me to work hard from the first day. Thanks to her, I have a thesis that I am very proud of.

John Krogstie has been my advisor at the Department of Computer and Information Science (IDI) at NTNU, and his acceptance of the project proposal has made it possible for me to work on a topic that I find very interesting.

The findings in this report were made possible by the contributions of 14 anonymous participants, who were willing to talk openly about the challenges in their field. I thank them for their time, contributions and honesty.

The last year at NTNU I have been so lucky as to share an office with Kristine Steine, Tibor Vuković and Juul Arthur Ribe Rudihagen. Their support, laughter and friendship have made working on this thesis a lot easier.

Saving the most important for last, I thank my wonderful parents who have thought me the value of learning, hard work, and encouraged my curiosity. Their guidance and support for everything I do have given me a better start in life than anyone could have asked for.

Finally, I thank Hilde - my girlfriend - who has been a wonderful support throughout the last year, encouraging me to keep going, accepted my late hours, and helped proofread the thesis. With humour and intelligence, she has brought me joy beyond what I deserve, and I could not be happier.

”There is no wealth like knowledge, no poverty like ignorance.”
- Ali

Hans Kristian Henriksen

Hans Kristian Henriksen

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter introduces the study conducted into the security requirements in Norwegian public procurements. A background for the study is given in Section 1.1. Section 1.2 presents the research questions set for the study, while Section 1.3 outlines the methods used to answer the research questions. In Section 1.4, the privacy of the participants, and how this was ensured is discussed. Finally, Section 1.5 presents the outline of the rest of the thesis.

1.1 Background

Whenever the Norwegian government intends to acquire products or services with an estimated cost of more than 500 000 NOK[1], a procurement process must be started [2]. As part of this process, a request for tender is published, available for answer by all, or a selected group of, qualifying businesses. The tender specifies a set of selection criteria and their importance. Based on this, the supplier that best fulfils the criteria wins the bid, and is allowed to deliver the product or service.[2] [3]

When a tender is published, the purchaser can no longer make significant changes to the tender documents that have been published. Consequently, all documents must be carefully reviewed before they are released. New information may not be possible to include into the tender without cancelling the competition, and then announcing a new one. This is time and resource intensive, and can seriously delay the procurement of the system or service in question.

[1] There are a number of exceptions to this rule, none of which are further discussed in this report.

[2] This is obviously a simplification of the more than 25 000 word regulation that governs this area, but it is sufficient to give an introduction to the procurement process. The process is further discussed in Chapter 2.

With the public procurement process not lending itself to changes, system requirements must be clearly formulated before the system is procured. Security must then be very clearly reflected upon before the tender is presented if specific requirements are to be given in the tender. A question then arises; what is the state of security requirements under these kinds of restrictions, and what improvements can be made to the current situation?

There seems to have been little research in this field. The most relevant work has been done by Lauesen [4, 5], and Moe and Päivärinta [6], who have looked into requirements *in general* in connection to the procurement processes. Neither address security requirements specifically.

This thesis consists of two main parts. The first contains an overview of the procurement process used in Norway, and a summary of the prestudy conducted in the fall of 2015. The prestudy contains a literature review on the subject of security requirements in public procurements, as well as an examination of 29 tenders for IT-systems given by the Norwegian government.

The summary of the prestudy presents the current state of the practice of security requirements in Norwegian public procurements, and compares it to the recommendations given by both the literature, and three of the largest security standards, *ISO 27002*, *Common Criteria* and *PCI-DSS*.

The second part of the thesis is based on the outcome of the prestudy. As was found in the prestudy, there is a large gap between the recommendations given in the literature and the actual requirements given for security in tenders. Based on that knowledge, this thesis continues the path towards understanding the security requirements, and how these are affected by the procurement process. To explore this, an interview study is conducted, consisting of a questionnaire and a set of semi-structured interviews.

1.2 Research questions

To be able to investigate the processes of designing and implementing security requirements, the following research questions have been identified.

RQ1 How is the current state of security requirements in public procurements viewed by procurers and suppliers?

RQ2 What challenges exists when procuring IT-systems, and how does this affect security requirements?

RQ3 What recommendations can be given to improving the current state of security requirements in public procurements?

The prestudy found that there are variations in the quality of security requirements set forth in public procurements, and that there are discrepancies between the recommendations in the literature and the current practice of security requirements. RQ1 investigates how the suppliers and procurers view the current state of security requirements in public procurements. While the prestudy found numerous areas where the state of practice appears to be out of line with the recommendations, it is possible that these problems are addressed in the procurement process, while not visible in the tender documents.

In order to be able to offer suggestions for improvements, there is a need to understand the challenges faced by the actors in the procurement process. This is put forth in RQ2, asking about the challenges that exists in the procurement of IT-systems. Gaining an understanding of these challenges will enable recommendations, as well as laying a foundation for further work in the field.

Together, RQ1 and RQ2 broadens our view from the prestudy and allows for a wider look at the public procurement process as a whole.

Finally, if this thesis is to have value for the stakeholders in the procurement process, there must be some recommendations for best practices or methods. This is posed by RQ3, which has the intention of identifying any recommendations that can be made to improve security in publicly procured IT-systems.

1.3 Methodology

In order to answer the research questions, a set of research methods were used. This section will briefly explain the literature review and document review used in the prestudy and the questionnaire and interview study conducted in the thesis.

1.3.1 Literature review

No literature in the specific field of security requirements in public procurements was found. There was some literature on the topic of requirements in public procurements, notably the research by S. Lauesen [4, 5]. Due to the lack of specific literature on the subject, it was decided to search for literature relating to security requirements and public procurements separately in order to get a better understanding of each field, and then attempt to put this information together. The study was conducted as a semi-structured literature review, searching the largest indexes of scientific research on the area, Google Scholar, Science Direct and IEEE Xplore, for relevant terms.

The main selection criteria for the articles was the content of the abstracts. Given an abstract that presented interesting findings, or related to the subjects at hand, the articles were further investigated.

1.3.2 Document review

The tender documents studied were retrieved through Doffin, the Norwegian database for public procurement. The search criteria set was that the system had to be categorised as part of the IT-sector, and the tender had to have been published within the last 12 months at the time of searching. Going through the tenders, the selection was done based on the tender fulfilling at least one of the following criteria:

- pertained to an interesting or clearly defined system
- was issued by a type of organization that was not yet represented in the selection
- was issued by an organization that is central in the Norwegian society

The goal was to gain a broad selection of organisations, tender types, and systems. In addition to these tenders, four tenders were provided by Lillian Røstad[3], as a result of her contacting her network for interesting tenders that may not have been available in Doffin.

1.3.3 Questionnaire

To understand the attitudes of the people involved in the public procurement process, a questionnaire was created to be sent to stakeholders on both the procurer and supplier side. The goal of the questionnaire was to gather information about who the participants were, understand their thoughts on security requirements and the recommendations identified in the prestudy, and provide an opportunity to plan each interview individually. The questionnaire included security requirements engineered to contain flaws in accordance with the findings of the prestudy, and asked about attitudes towards the themes of these recommendations.

A digital survey tool was used to conduct the survey in order to be able to use skip patterns and automatic analysis of the results. This also removed the risks of surveys getting lost in the mail, and the need for digitalisation. In accordance with recommendations in the literature, the survey was

[3] Lillian Røstad has been the external advisor for both this thesis and the prestudy. During the period of this work she has had a position as department head at Difi, and is now employed as the security lead at Sopra Steria Norway.

designed to capture and keep the attention of the participants by placing simple questions at the beginning, advancing to more difficult questions, and then concluding with something of interest.

1.3.4 Semi-structured interviews

A set of 12 semi-structured interviews were conducted in order to understand the process leading up to the security requirements in the tenders issued by the public, and their interpretation by the suppliers. It was decided that a semi-structured approach would be best suited, as the author's knowledge of the field is quite limited compared to the participants', thus providing the needed flexibility to follow up on interesting and new information provided by the participants.

To facilitate the interviews, an interview guide was developed, structured in the same way as the questionnaire, with fitting probes for each question. In line with the recommendations of the theory, the interviews start with easy questions meant to get the participants to talk freely, and build rapport with the interviewer, advancing to more difficult topics later. The interviews are finished off by asking the participants to offer their thoughts on any uncovered topics, as well as opening for questions.

1.4 Privacy

Throughout the work on this thesis, the ethics, and specifically the privacy of the participants, has been central. Interviewing people about themes related to security is sensitive. Both for the security of the people and companies involved, and to make sure that participants were not discouraged from volunteering for the survey, privacy concerns were put front and centre from the beginning of the project.

As information such as names, emails and, due to the questionnaire, IP-addresses had to be collected, laws on data collection become relevant. The project is bound by §31 of the Law on the Processing of Personal Information, which requires any project processing this kind of information to report it at least 30 days before collecting data [7]. NTNU uses the Norwegian Social Science Data Service (NSD) as their data protection official. Because of this, there is not only a duty to report the project, but an application that must be approved before collection of data can start. This adds to the time taken to be able to start data collection, as NSD estimates 6 to 8 weeks to approve projects. The study was approved by NSD, and assigned project number *46907*.

The privacy of the participants has been ensured through the use of anonymous identifiers. Each participant has been assigned a random string of characters that has been used instead of their name on all documents and recordings. The key translating these strings to the identity of the respondents has been kept locked away from the rest of the research material. In addition, no information about the participants, other than the fact that they work as a procurer or a supplier, is described in this report.

The law requires the participants to give their informed consent to participate in the study. All participants were informed about the privacy measures taken, and the way the study would be conducted before they were asked to answer the survey. This information was given along with a consent form (presented in Appendix C), and the participants were reminded of the central points of the consent form before the interview started. By handing in the questionnaire, the participants agreed to the collection of the survey data, and this was clearly stated at the beginning and end of the questionnaire (given in Appendix A).

The subjects covered in this report is by many regarded as sensitive, and great care has been taken to ensure that no information can be traced back to a person, system or employer.

1.5 Outline

Chapter 2 gives an overview of the public procurement process, and the potential challenges it poses to development and implementation of security requirements. In Chapter 3, a summary of the prestudy that was conducted in the fall of 2015 is given. Chapter 4 provides the experiment setup, describes the creation of the questionnaire and interview guide, and the actual conduction of the experiment. The results and recommendations are given in Chapter 5. Finally, the conclusions are presented in Chapter 6, along with recommendations for further work.

Chapter 2

Public procurement

The public procurement process is a complex legal field which could be the subject of several master's theses of law. It is not the goal, nor in the scope of this thesis, to venture into the finer details of procurement law. The overview of the laws and regulations that govern public procurement will therefore be quite short and general. This chapter is meant as a simplified introduction to the laws and regulations, and should not be seen as legal advice. Most of the chapter is a reproduction from the prestudy [1]. It has been included as it is essential background information needed to understand the rest of the thesis.

2.1 Goal of procurement

The act of public procurement stretches far back in history, with one of the first recorded instances being from Syria about 2800-2400 B.C. The goals of procurement vary with the situation of the country that is studied, but for most countries the central goals are to get products of high quality, at low cost, delivered in short time. Procurement (i) raises the competition level in the market, (ii) encourages innovation, (iii) can force environmental and social goals, and (iv) ensure fair competition amongst different suppliers. [8, 9]

The Norwegian Law on Public Procurement states in the first section that the goal of the law is to *"ensure the most efficient resource use possible"*. [10]

2.2 Regulation

Public procurements are regulated through Law on Public Procurement [10], and Regulation on Public Procurement [3]. As part of the European Economic Area, Norway is bound by the European laws in this field. These have been incorporated into the Norwegian laws, and all procurements that exceed the EU threshold level are bound by the same laws as in the rest of the EU. [11]

2.3 Competition types

When publishing a tender, there are four types of competitions that can be used. The competition type regulates how the process is conducted, what communication is allowed between the parties, and who can be qualified to bid on the tender. Depending on the tender, not all competition types may be allowed, and some will be more fitting than others. Below follows a short description of each competition type.

2.3.1 Open competition

In an open competition, all suppliers may provide an offer to the published tender. The purchaser may set requirements for qualification, and all suppliers that fulfil these will have their offer evaluated. There is no room for negotiation in this form of competition, meaning that all requirements must be written with great care. Once the competition has started, there is little room for changes to the tender documents. [12]

2.3.2 Restricted competition

A restricted competition resembles an open competition, but allows the purchaser to limit the number of suppliers who are allowed to give an offer in response to the tender. This is useful in situations where the purchaser expects to receive a large number of offers. A pre-qualification is held to select the suppliers who are allowed to make an offer. There is no room for negotiation in this type of competition. [12]

2.3.3 Competition with negotiation

In a competition with negotiation, there is room for the suppliers to improve their offer based on conversations with the customer. Based on the monetary size of the tender there may be two phases, where the first is used to qualify the suppliers that are to be allowed to deliver an offer, the same as in a restricted competition. The second phase is negotiations, which follow strict rules to ensure that no suppliers are discriminated against. During the negotiations, the suppliers are informed of the strengths and weaknesses of their offer, and given the opportunity to make clarifications and have their questions answered. [13]

Competition with negotiation is seen as a resource intensive competition form, as the purchaser has to engage in negotiations with a potentially large group of suppliers. It can also be difficult to satisfy the non-discrimination rules of the negotiations, risking cancellation of the tender. [13]

2.3.4 Competitive dialogue

Competative dialogue is only allowed if the tender is regarded as *especially complex*. This is the case if the purchaser can not objectively define the requirements for the system, or is not able to objectively define the judicial or financial conditions of the project [14]. Suppliers are invited to be qualified, and there may be a limitation on the number of suppliers that are allowed to present an offer. Through dialogue with the different suppliers, the purchaser attempts to find an unambiguous description of the product to be purchased. Once such a description is found, the negotiations are ended, and the suppliers are asked to answer a tender based on the solution found in the negotiation phase. [15, 16]

2.4 The procurement process

Procuring a product or service is a long process, which involves several steps. A short overview of the process is given in figure 2.1. Based on [17] the process can be summarised as follows:

After identifying a need for a product or service, the organisation will usually do some internal work to plan the procurement. The real needs of the organisation are identified, as well as exploring any alternatives to starting a procurement process. Given that a procurement process will be necessary, preparations for the tender starts. One of the competition types described in Section 2.3 must be chosen, along with the rules for the competition. The necessary documents must be prepared, including the contract to be signed, all requirements for the system, qualification requirements and so on. This is published in the national database for public procurement (Doffin) if the estimated cost is above the national threshold, and in the equivalent European database (TED) if the estimate is above the current EU-threshold. The competing companies can ask questions during the competition period, and clarifications may be made to the tender.

After the deadline a supplier is chosen based on the award criteria, and announced as the winner. Given that there are no complaints (in 2015, The Norwegian Complaints Board for Public Procurement (KOFA) processed 181 complaints regarding procurement processes [18]) the contract can be signed, and delivery can start. The last phase is to ensure that the correct product is delivered, make payment, and conclude the contract.

This thesis focuses on phases 3 through 6 of Figure 2.1. The prestudy investigated phase 4 and looked into and analysed the actual published documents from tenders. The study conducted in this thesis attempts to explain these findings by investigating the phase leading up to the tender documents (phase 3), the phase where documents are published and questions answered (phase 4) and the phases where the documents are interpreted and the system is delivered (phases 5 and 6).

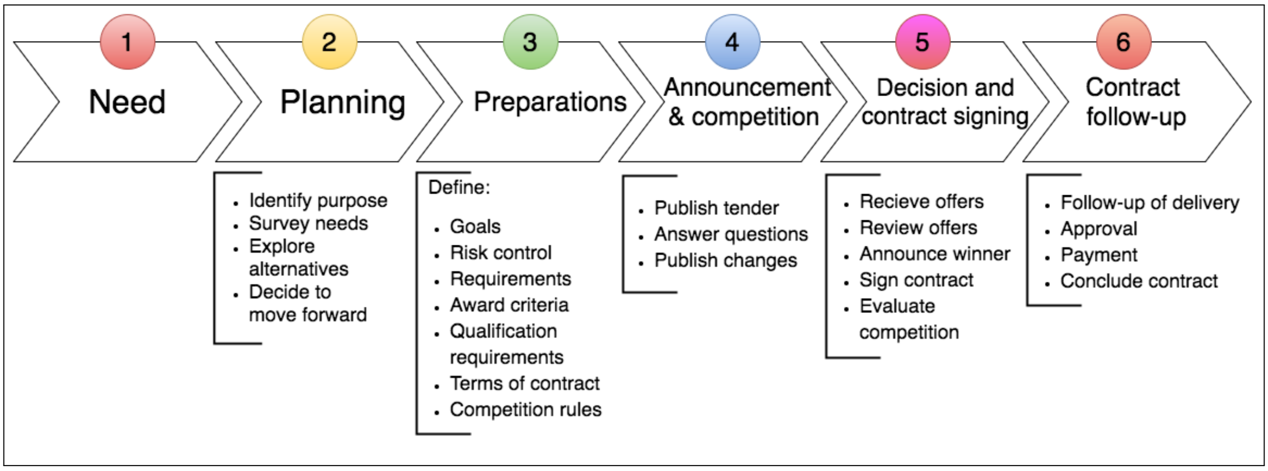


Figure 2.1: Simplified view of the public procurement process, based on [17]

2.5 Challenges in public procurements

One of the central factors separating the public procurement process from how a private company would acquire a new system, is the inflexible nature of the tender. Once the tender is published, the contents can not be changed [4]. Therefore, all requirements must be well considered before the tender is put forth [19]. If a competition with negotiation or competitive dialogue is used, there is more room for changes, but the tender documents are still important in specifying the system that is to be purchased.

To overcome some of the challenges connected to the inflexible nature of the tender, the suppliers are allowed to ask clarifying questions to the content of the tender documents. There are however strict rules governing the answers that can be given, to ensure that the purchaser does not use the questions to alter the meaning of the tender documents. In addition, the questions and their answers are made available to all other suppliers to ensure a fair process. The transparency is a deterrent to asking questions, as it might reveal parts of the offer a supplier wants to submit. [20]

These inflexibilities affect security requirements, as changes to security must often be done based on the fluctuations both of the system and user needs, but also because of the constantly evolving technology. This is central to the challenges looked into in this thesis.

The limitations of the public procurement process motivate the identification of recommendations that can be given for writing security requirements, as asked in RQ3 (Section 1.2). To be able to answer this, there is a need to understand how the procurers and suppliers view the procurement process, and how security requirements are affected by the procurement process. This is facilitated by RQ1 and RQ2.

Looking back on the phases of Figure 2.1, the prestudy covered step 4 in great detail, though on a theoretical level. This thesis will investigate phases 3 through 6, focusing on the views of the people actually experiencing and participating in the procurement process. Together with the findings of the prestudy, this should help gain an understanding of the challenges faced, and how these are best solved.

Chapter 3

Prestudy

This chapter gives an overview of the prestudy conducted by the author in the fall of 2015, titled *"Security Requirements in Norwegian Public Procurement"* [1]. The prestudy was conducted to get a better understanding of the state of security requirements in Norwegian public procurements, as well as to gather research literature on the subject. It has been described here to provide background for the thesis, as the conclusions from the prestudy are the basis for the questions posed to the participants in both the questionnaire and interviews (described in sections 4.2 and 4.3).

The chapter starts off with the research questions, problem description, as well as background for the study in Section 3.1. In Section 3.2 the methods used in the prestudy are outlined, followed by a summary of the literature and document reviews in Sections 3.3.1 and 3.3.2. Lastly, the conclusions and limitations are presented in 3.4.

3.1 Problem description

The prestudy was based on a problem formulation put forward by Lillian Røstad, then department head at Difi, now Security Lead at Sopra Steria Norway.

> *As the use of IT-systems in all parts of society is increasing, so is the need for information security, both in private and public sector. The task is to look into current research on requirements for information security, how these requirements are set, and attempt to give recommendations about how it should be done, in what areas requirements should be set, etc.*

The problem description was motivated by a wish to evaluate the security requirements given in public procurements of IT-systems. According to numbers from 2012, the Norwegian government uses approximately 20 billion NOK[1] every year procuring IT-systems and services [21]. With such large sums of money being used on important, and sometimes critical, IT-projects, it is vital to understand the quality of the security requirements that are set.

Evaluating tenders given in the near past is central in order to understand which requirements are set for security, and to contribute to the improvement of security requirements given. The ultimate goal of the prestudy was to provide the foundation for a structured and focused effort to improve future security requirements, not to simply point out flaws in the current state of affairs.

3.1.1 Research questions

The prestudy attempts to answer the problem description setting forth three research questions:

RQ1 Which information security requirements are set by the government when acquiring IT-systems?

RQ2 What does the theory say - what recommendations for defining requirements when acquiring IT-systems exists?

RQ3 What is the gap between recommendations and reality - is there a large deviation or a large correspondence?

3.2 Method

Based on the research questions identified in Section 3.1.1, two methods were found necessary to be able to provide answers. RQ2 and RQ3 relate to the existing literature in the field, making a literature review necessary. RQ1 and RQ3 require knowledge about the current state of affairs of public procurements in Norway. The best way to gather objective and verifiable information about this is through the tender documents that are published to the suppliers. A document review of a selection of these documents can be used to answer these questions.

3.2.1 Literature review

Starting out, my advisor was not aware of any specific research into the field of *security* requirements in public procurements. Initial searches for theory in

[1] Neither Difi, nor Statistics Norway (SSB) were able to provide any newer or more reliable numbers.

this field did not yield any results. There is of course ample research in both the fields of *security requirements* and *public procurement*, but there seems to be a lack of research connecting the two fields. Due to time constraints, and the fact that the amount of possibly relevant literature was large, an unstructured approach was used in the literature review. Literature about the two separate fields of research was gathered and organised according to the overall theme of the study. The goal was to reach some kind of information saturation, where new documents on the subject provided little or no new information. Using search terms such as *computer (procurement OR tender)*, *requirements (procurement OR tender)* and *requirements engineering acquisition*, Google Scholar, Science Direct, and IEEE Xplore were searched.

3.2.2 Document review

The tender documents were collected from Doffin, the Norwegian database for public procurement, which contains the tenders for all publicly available procurements.[2] In some instances, the tender documents were directly available from Doffin. If this was not the case, the government agency responsible for the procurement was contacted, and requested to provide the documents in accordance with the Act relating to the Right of Access to Documents Held by Public Authorities and Public undertakings - the Norwegian Freedom of Information Act (Offentleglova)[22].

To facilitate the analysis of the tender documents, a working definition of *security requirement* had to be made. The literature makes it clear that this is no easy task, summarised nicely by [23] in their survey of techniques for eliciting security requirements:

> "(...) we haven't found a universally accepted definition of "security requirement" in the literature."

Risking missing relevant requirements if the definition was too restrictive, the definition is based on what the procurers have defined as a security requirement. This decision was based on the argument that the suppliers have been tasked with implementing the requirements as security requirements, making them *de facto* security requirements, even if one could argue strongly that the requirements are not primarily security related. In addition, requirements that describe a security policy, constrains the system's functionality for security or privacy reasons, and requirements that fit into one of the categories identified in 3.3.1.8, has been regarded as security requirements.

[2] If a call for tender is published to a limited group of suppliers, e.g those part of a framework agreement, the call for tender is not necessarily published in Doffin.

3.3 Results

3.3.1 Literature review

The literature review of the prestudy concludes with seven main recommendations for writing security requirements, briefly presented in Sections 3.3.1.1 through 3.3.1.7.[3] Section 3.3.1.8 presents ten categories of security requirements made from the recommendations of *ISO27002*, *Common Criteria* and *PCI-DSS*.

3.3.1.1 Gather security requirements in one place

As tenders can have large amounts of requirements, it is recommended that the security specific requirements are gathered in one place in the requirement documents. This can be hindered by tenders where the requirements are split between several documents due to laws and regulations.

3.3.1.2 Security requirements should not place unnecessary constraints on the system

Requirements that specify technology too exact, may hinder good security as more relevant or updated technology may be available. Since the requirement specification becomes part of the contract, this can legally stop the supplier from giving the best possible security, or disincentivise suppliers from taking part in the bid.

3.3.1.3 Security requirements should not be too open or vague

The opposite of the previous point is requirements that are difficult to implement because they are too vague. Considering the short window that is given to answer the tender, it can be difficult to interpret what the customer really wants in the time allotted. One way to clear this up is through asking questions to the customer, but as these are public, the supplier risks revealing business secrets or parts of their bid.

3.3.1.4 There should be a consistent selection of security requirements

Security requirements usually make implications about what is important assets, or focus on security. Stating that data should be encrypted in transport, implies that the data is valuable and should be protected. It is then important that this is reflected in the rest of the security requirements, such that

[3] The order the recommendations are presented in is extraneous

the rest of the requirements reinforce this implication. Following the above example, we would expect to see requirements for encryption of databases, physical security and so forth.

3.3.1.5 There should be a consistent level of detail in security requirements

To ensure that some security requirements are not viewed (wrongly) as being more or less important than others, procurers should strive to produce security requirements at a consistent detail level. Inconsistent detail level will typically arise when the requirements are written by a so-called *local heroes*, who are knowledgeable in some fields, but not in all the security fields needed for the system.

3.3.1.6 Requirement documents should not be too large

It is recommended that the requirement documents, including the security part of these documents, should not be too large. The risk is that some parts of the documents might be missed or skipped.

3.3.1.7 Well known standards should be followed

As security is a complex field that is difficult to do right, a single organisation should not expect to be able to cover all security in their requirements. Following popular and regularly reviewed standards for security requirements, as well as requiring suppliers to comply with international standards for secure development, improves the likelihood that the security requirements and the security of the system will be of high quality.

3.3.1.8 Standards

In addition to the review of the literature on the subject of security requirements, three well-known security standards were reviewed in an attempt to find similarities that could be used for both analysis and recommendation. The standards in question were *ISO27002*[24], *Common Criteria*[25] and *PCI-DSS*[26]. These standards have slightly different areas of use and main focuses, which was considered as positive given the wide spread of systems being procured by the government.

Below follows a short description of the standards. A more thorough description is provided in [1].

ISO 27002 This standard is part of the ISO 27000-series, a set of standards that focus on security in information systems. While ISO 27001 pertains to the implementation of an Information Security Management

System (ISMS), and can be relevant to require from the suppliers, ISO 27002 describes concrete security controls which can be implemented to mitigate different risks. The standard lays out a total of 114 controls, sorted into 14 clauses.

Common Criteria Being a standard for security certification, Common Criteria (CC) can nonetheless be used to learn about different ways a system can be protected, and steps that should be taken in securing data. Through the use of general *protection profiles*, CC makes it possible to generalise systems, giving a starting point for specifying security requirements. CC outlines 11 classes of security objectives that should be considered when risk assessing a system.

PCI-DSS As an industry specific standard, PCI-DSS has value also for generic systems, as it is the standard of one of the most risk averse and security seeking businesses in existence; the payment card industry. Aimed at any business handling card data, the standard is developed to be easy to understand and implement. The standard presents 12 main requirements and gives detailed instructions for their implementation and testing.

Common for all these standards is the fact that they should not be implemented uncritically, but rather as a part of a cost-benefit analysis, and after identifying the critical assets that are to be protected.

From the standards, a set of common areas can be identified, and these are shown in Table 3.1. The areas are a result of categorising all requirements and recommendations from each of the three standards, and attempting to condense these down to a small number of categories. To accommodate the differences between the standards, the categories have been given other names than they might have in any of the standards, and some of the categories are quite vague. An explanation of the categories of Table 3.1 is given in Table 3.2.

Table 3.1: Common categories for security requirements

Category	**Examples from category**
Cryptography	Encrypt data on open networks [*] Key management[†] [‡] Modes of operation[†]
Protection of data and assets	Handling of assets[‡] Transport of assets[‡†]
Operations security	Protection from malware and viruses[*‡] Backups[*‡] Logging[*‡]
Authentication of users	User Authentication[*†‡] User Identification[†‡] Revocation and expiration[*†‡]
Incident management	Intrusion detection[*‡] Reporting of security events[‡]
Physical security	Detection of physical attack[†] Secure areas[*‡]
Audit and testing	Audit of system security[*†] External testing[*] Audit trail[‡]
Security focus during development	Keep systems up to date[*‡] Change control[*†]
Organization security policy	Information security policy[*‡]
Compliance	Compliance with laws and regulations[‡]

[†] Common Criteria
[‡] ISO 27002
[*] PCI-DSS

Table 3.2: Explanation of the common categories for security requirements

Category	Explanation
Cryptography	Concerns the encryption of data that is to be kept secure. Especially relevant for data transport on networks. Also includes key management throughout the life cycle of the key.
Protection of data and assets	Regards the entire lifespan of assets, how are they stored, managed, protected, accessed, used, sent and destroyed.
Operations security	This encompasses the operational procedures of the system. Making sure that the system is running correctly, having adequate backups and roll-back routines. Keeping up to date logs of the system, and their use is also part of this.
Authentication of users	All activities related to the identification and authentication of users. Includes handling of user rights, de-authentication and corresponding routines.
Incident management	Routines and requirements for responding to incidents that have happened. Includes detection, analysis, countermeasures, forensics and reporting.
Physical security	Everything related to the physical environment the system operates in. Access control, fire safety, camera surveillance and on-site guards are examples of physical security measures. In addition, routines for preventing, detecting and handling physical attacks are included.
Audit and testing	Having requirements and routines for auditing the system's security, and making the system easy to audit. Tests can be performed both by external and internal testers.
Security focus during development	Keeping systems and dependencies up to date, making sure that the latest security patches are in use. Employing a change control system to make sure that all changes are approved, audited and documented. Also includes making sure that security is an area of focus during development.
Organisation security policy	This category concerns the existence, content and updating of a security policy for the organisation as a whole. How are employees supposed to handle sensitive materials, and what rules and policies make sure that employees act in a manner that is supportive of information security are part of this category.
Compliance	This category pertains to compliance with current laws and regulations, as well as industry-specific requirements. Compliance with concrete technical requirements that are given by lawmakers or others is also included.

3.3.2 Document review

The 29 studied tenders were analysed for security requirements in an attempt to understand what parts of software security the requirements cover, and to

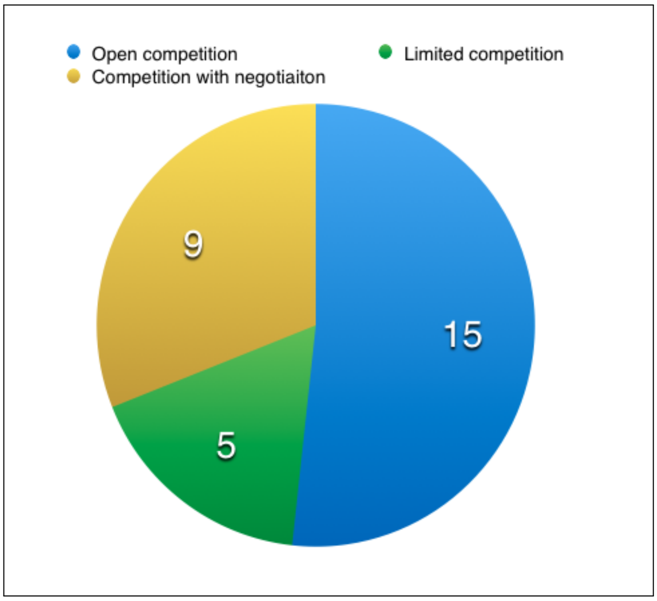


Figure 3.1: Summary of competition types in selected tenders

understand if there are any connections between security requirements and other parts of the tender. Eleven of the tenders were given by municipalities or county municipalities, and 18 were from various governmental organisations. The average system cost (bar one outlier) was 10 million NOK, 24 tenders were for the purchase of an IT-system, while 5 were tenders for the purchase of competence. The distribution of competition types in the selection is given in Figure 3.1.

Section 3.3.2.1 will present the data analysis done on the tenders, highlighting connections between tender size, number of requirements, system cost, and the number of security requirements. In Section 3.3.2.2, the recommendations identified in Section 3.3.1 are revisited, and exemplified by findings from the studied tenders.

3.3.2.1 Data analysis

To understand the selected tenders, several aspects of the tenders were analysed. Figure 3.2 shows how many security requirements were present in the requirement specification of the tenders. In Figure 3.3[4] the total number of

[4] The author was provided with the full requirement specification for 27 of the 29 studied tenders. These are the ones showed in the figure.

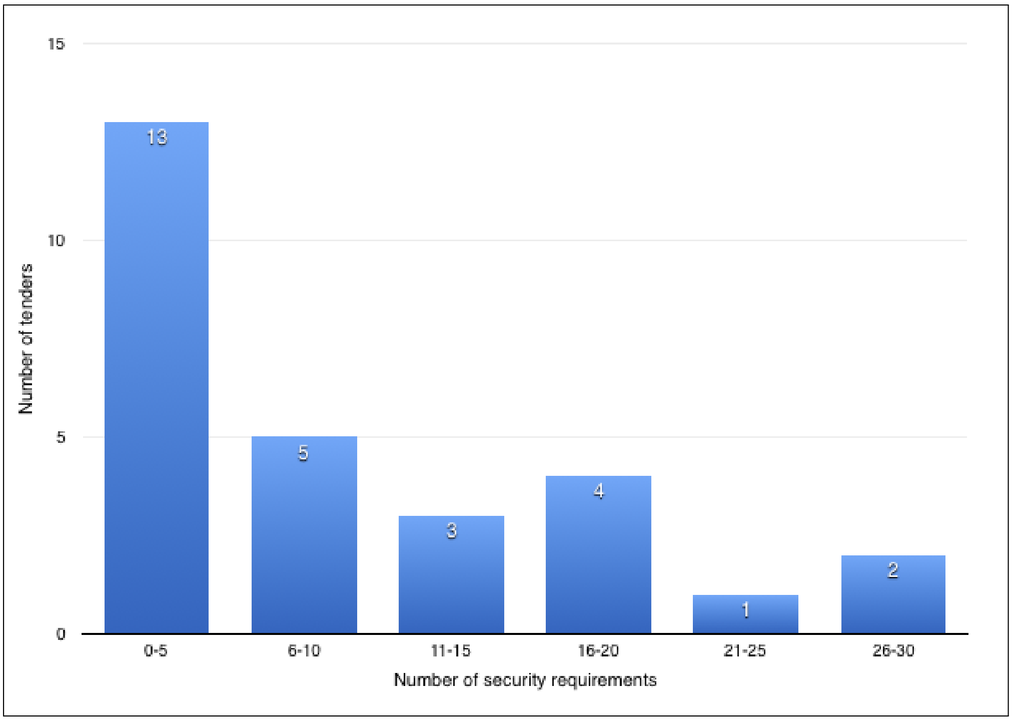


Figure 3.2: Histogram of the number of security requirements per system

security requirements are plotted against the total number of requirements[5]. In Figure 3.4 the total number of security requirements are plotted against estimated system cost[6].

From Figure 3.3 it can be observed that there appears to be a positive correlation between the number of requirements and the number of *security* requirements. System cost does not seem to affect the number of security requirements, though there are too few tenders providing a cost, and the cost spectre is too large to be able to draw any conclusions.

[5] Some tenders have optional functionality which the supplier may choose to implement. This has been included in the total number of requirements, as it is expected that the security requirements also cover these optional parts of the system. For tenders including more than one contract (e.g. both development and operations) all requirements from all contracts have been counted.

[6] Only 20 of the studied tenders provided a cost estimate. Where a minimum and maximum value was provided, the average is used. One outlier has been removed, being more than 30 times larger than the average system cost.

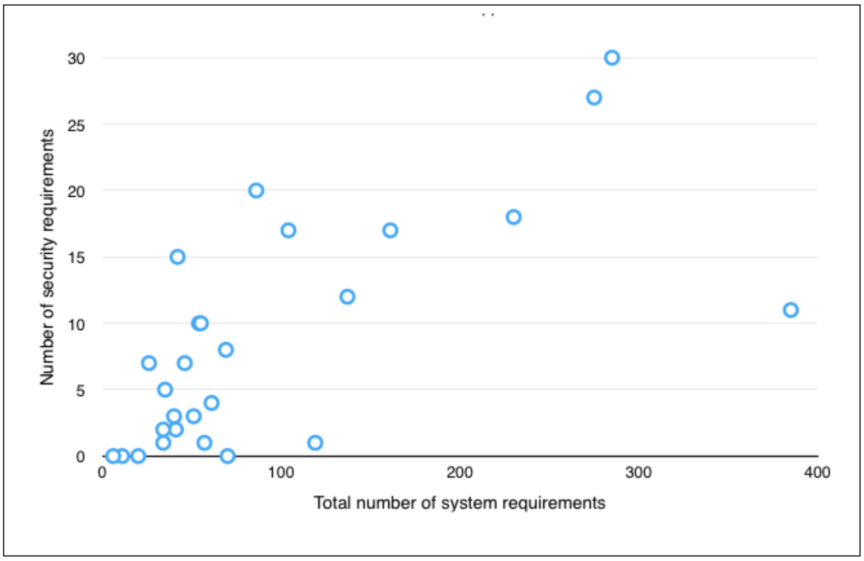


Figure 3.3: Number of requirements plotted against number of *security* requirements

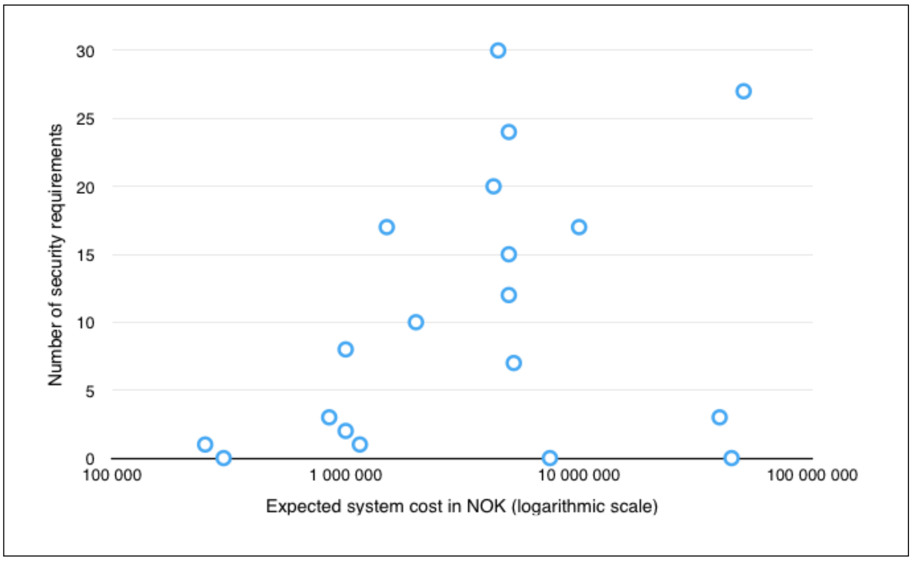


Figure 3.4: Number of requirements plotted against estimated project cost

3.3.2.2 Literature recommendations

Looking into the literature recommendations from Section 3.3.1, it is possible to find good examples from the studied tenders for each recommendation. In this section, a quick insight is given, while more in-depth results can be found in [1].

Gather security requirements in one place It was found that most of the tenders with a high number of security requirements placed them under a separate security heading, though there were usually some security related requirements under different headings. There were several tenders where the security requirements were spread throughout the specification, and numerous examples of security requirements being placed under headings making them seem unrelated to security.

Security requirements should not place unnecessary constraints on the system Several examples of tenders requiring very specific technology, or in other ways placing strict constraints on the system were found. The general impression was however that procurers are not placing unnecessary restrictions on the systems. Some exceptions that seem related to laws and regulations were found, though this is not something the procurers can be held accountable for.

Security requirements should not be too open or vague Vague requirements are either too broadly defined to be answered in a satisfactory manner, or they open the possibility of the supplier delivering a sub-standard solution that legally complies with the requirements, without actually solving the customer's problem. Especially requirements containing qualitative statements are prone to be too vague, and several examples of this were found. There were also several instances of requirements that simply put the burden of making the system secure on the supplier, without specifying what security was needed.

There should be a consistent selection of security requirements It appears that making a consistent selection of security requirements is a challenge. In the studied tenders, there seem to be deviations from what one would expect, with e.g. 22 systems having authentication requirements, but only 13 having requirements in cryptography, and a mere 6 having requirements in physical security. This suggests a situation where there is data that should be guarded against unauthorised persons, but that is not protected in transit or storage.

There should be a consistent level of detail in security requirements An inconsistent detail level can be thought of in several ways. One can look at the number of requirements for each area of security, at the detail level from requirement to requirement, or the difference in detail between security requirements and other requirements in each tender. For the first of these, there was evidence of inconsistencies, with some tenders having many times more requirements in some categories. The detail level of security requirements seems to be consistent within the studied tenders, while there was not sufficient time to investigate the relative detail level of security requirements against the nearly 2500 total requirements in the selected tenders.

Requirement documents should not be too large The size of the requirement specifications has been a hugely varying factor in the studied tenders, ranging from 6 to 385 requirements. As shown in Figure 3.3, there are few tenders with more than 100 requirements, and for some of the larger specifications, it became difficult to ensure that all security requirements were identified, due to the size of the document. This exemplifies the risk presented in the theory, that large requirement documents increase the risk of missing security requirements.

Well-known standards should be followed The use of some sort of standard was required by 18 of the studied tenders, including locally developed standards. For the remaining requirements, several attempted to impose some sort of standard on the supplier by generic statements such as *"(...) must be in accordance with current standards for system architecture and security"*. The tenders that did refer to recognised standards mainly focused on ISO 27001, standards developed by the Norwegian National Security Authority (NSM) and OWASP Top 10.

Standards Looking at all the security requirements in the studied tenders, they can be sorted into the ten categories of security requirements identified in Section 3.3.1.8. The result can be seen in Figure 3.5, which shows how many tenders had at least one requirement in the different categories.

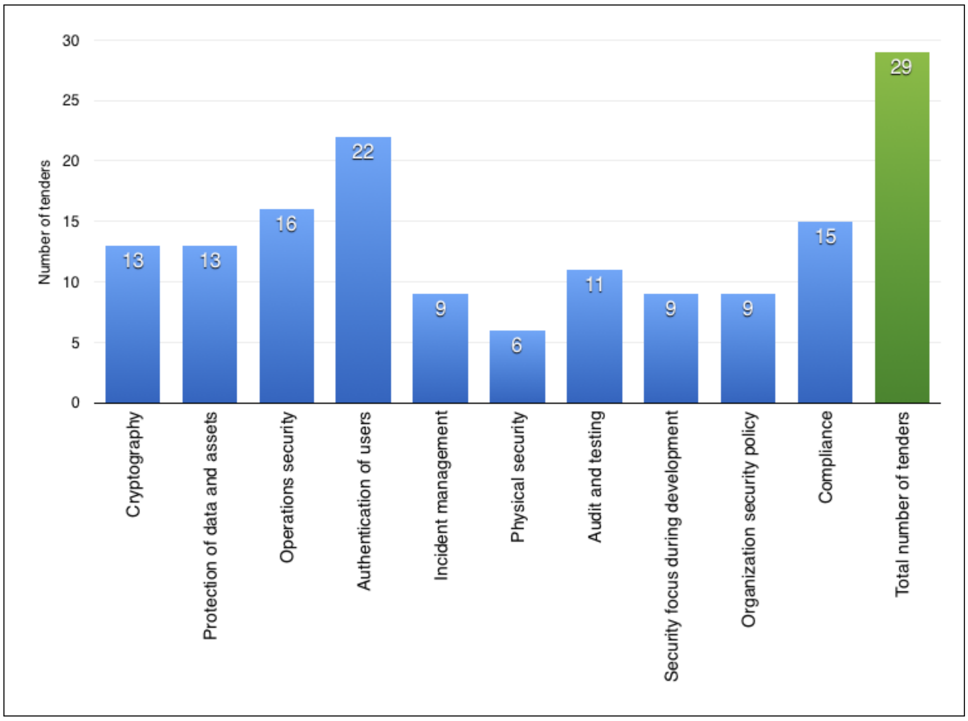


Figure 3.5: Number of tenders with at least one requirement in the given category

It is clear that no categories are taken into account by all the tenders, and most are covered by less than half. The top category is authentication of users, which was usually requirements for user login. Operations security comes in second place, mostly due to widespread requirements for some kind of logging. This is seen in connection with the third place, compliance, as many of the compliance requirements must be controlled by some kind of log system.

3.4 Discussion

The prestudy finds that the literature has seven main recommendations:

- Security requirements should be gathered in one place.
- Security requirements should not place unnecessary constraints on functionality.
- Security requirements should not be too open or vague.
- There should be a consistent selection of security requirements.

- There should be a consistent level of detail in security requirements.
- Requirement documents should not be unnecessarily large.
- Well-known standards should be followed.

In addition, the ISO-27002, Common Criteria and PCI-DSS standards were analysed, and a common ground of 10 categories from the standards were identified:

- Cryptography
- Protection of data and assets
- Operations security
- Authentication of users
- Incident management
- Physical security
- Audit and testing
- Security focus during development
- Organisation security policy
- Compliance

It was found that there are problems relating to most of the recommendations in the selected tenders. The most concerning finding is the lack of requirements for the suppliers to use any recognised standard for security in their work, as well as the apparent lack of consistency and coverage of the ten identified security areas. Only 18 of 29 tenders required the suppliers to adhere to some kind of security standard in their work with the software or service that was to be delivered. Covering all the security areas which were identified in the study was done by none of the tenders, but some were much better than others. Full coverage will not make sense for some systems, but it is highly unlikely that any system can be secure while covering only a few of these areas - as most systems are in some way accessible through the internet. No correlation between high quality security requirements and system size, cost, or organisation size or type was identified, though some correlation between the number of security requirements and the total number of requirements was found. It appears that local factors are deciding in the quality of security requirements, making the security of our critical public IT-infrastructure depend on the existence of *local heroes*, employees with a special interest for security, or a small part of the organisation that goes above and beyond to ensure security. This is however not enough; there is a need for highly educated and focused security personnel to keep up with the ever changing threats of the security world.

3.4.1 Limitations

This section presents the two main limitations of the prestudy, the selection of tenders for study, and the understanding of the law.

Tender selection Searching the governmental database for public procurement - Doffin - for all tenders put forth between 01.08.2014 and 01.08.2015 in all IT categories returns more than 500 results. With this kind of yearly volume, it was obviously impossible to go trough all documents. As described in Section 3.2, a selection of documents was chosen for review. This limits the applicability of the study, as results may be isolated to the selected tenders, and there might be interesting and relevant data in tenders not studied.

Understanding of the law Procurement law is a complex legal field, and as the author is not a lawyer, nor a law student, parts of the legal theory might have been misunderstood, in spite of the large amount of research done to understand the law.

Chapter 4

Experiment setup

This chapter describes the methods used in this study, the reasoning in choosing them, and their strengths and weaknesses. In addition, the conduction of the study is presented, focusing on the design and setup of the questionnaire and interview guide.

In order to answer the research questions given in Section 1.2, a mixed method approach was decided upon. There was a need for interviews with experienced people working with information security, in order to fully understand the challenges faced when procuring systems. At the same time, some information could be gathered faster with a questionnaire. Using both an electronic questionnaire and interviews, the data needed could be collected in an efficient manner.

Figure 4.1 gives an overview of the process that was used to conduct the experiment. The first activity was recruitment of participants, as conduction of the study was dependent on securing enough participants. While this process was ongoing, the design and setup of the questionnaire and interview guide started in parallel. These activities influence each other, as some questions from the questionnaire were found to fit better in the interview guide, and *vice versa*. After design and setup, both the interview guide and questionnaire went through testing, and the results of this was used in an iteration process to make improvements. The questionnaire was deployed after the testing was completed, and when the answers had been received, the results were analysed. These were used to make final refinements of the interview guide, and to make costum adaptations to the individual interview guides. When the individual interview guides were finalised, the interviews themselves were conducted, followed by the post-interview work of transcribing and coding the gathered data.

The chapter starts with a presentation of how the participants were recruited, given in Section 4.1. Section 4.2 presents the process of designing the

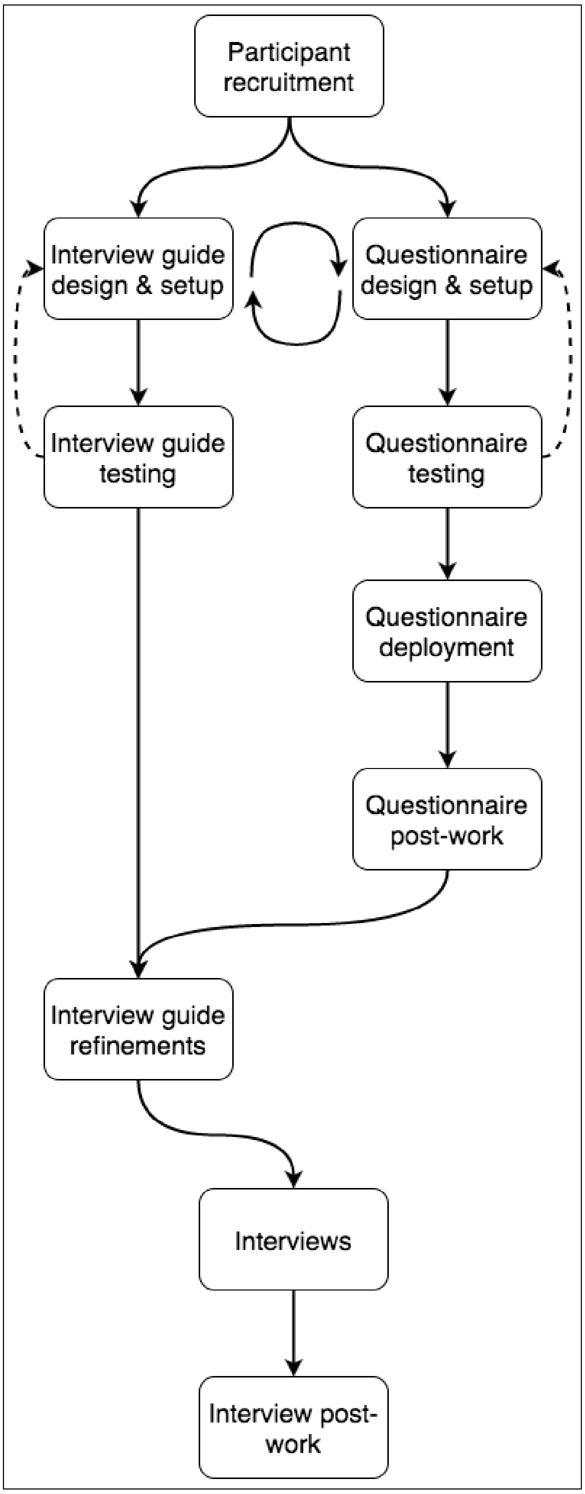


Figure 4.1: The experiment process

questionnaire, and the final questions that were sent to the participants. In Section 4.3, the interview guide is described, as well as the methods used during the interviews, and the planning of the post-interview work. The chapter is concluded with a discussion of possible alternative methods in Section 4.4.

4.1 Participant recruitment

Participant recruitment was one of the first activities conducted, as it was expected that this would be a difficult process. The study requires security operatives with years of experience to participate, people who are expected to have little time to spare. The ideal number of participants was set at somewhere between 10 and 20. This would allow an adequate selection of both procurers and suppliers, while taking into account that each participant added to the study adds to the time needed for both interviews, transcription and analysis of results.

The participants were recruited from the network of the author and Lillian Røstad, through the use of both direct emails to selected people and general calls for participants on the LinkedIn group of the Norwegian Information Security forum (Norwegian ISF). In total, 30 relevant people were identified through these recruitment techniques. Six of these were not contacted, either due to lack of up to date contact information, or a geographical location making it impractical to conduct an interview. Of the remaining 24, nine never responded to the emails with a request for participation, two stopped responding to emails during scheduling of the interview, and one declined to participate. This left 12 participants, giving an effective response rate of 50%.

Originally, the goal was to have one-on-one interviews with all the participants. Several of the participants did, however, want to have another person from their organisation present in the interview. To ensure their participation, this was accepted, though with a warning that some more time could be needed for the interview. This was not reported as a problem by any of the participants in question. As discussed in Section 4.3.3, not all appointments were carried out as planned, and some of the double interviews became single interviews. In the end, 14 people participated in interviews for this study.

4.2 Questionnaire

The use of a questionnaire was decided upon as one of the two primary data collection methods of this study. Firstly, since it was decided that face-to-face interviews would be needed, there was a need to collect some data about the participants. Additionally, it would be beneficial to be able to cut down the interview time by asking questions that could be answered just as easily in writing. The goal was to use the questionnaire as a means to support the interviews, by gaining some knowledge about the interview subjects beforehand, as well as helping the participants prepare for the interviews. Some questions, especially yes/no-questions, or questions where the respondents are asked to rate statements, can be asked just as effectively in a questionnaire as in an interview. Moving these questions from the interview to the questionnaire helps save time in the interview, which should be as short and efficient as possible [27]. Should any of the answers from the questionnaire be outside expected parameters, self-contradictory, or in disarrangement with the rest of the respondents, this can be followed up in the interview.

As the number of people answering the survey was not statistically significant, the data collected will not be reported directly. The main goal of the survey was to prepare both the participant and the interviewer for the interview, and the questionnaire results were mainly used to start discussions on the relevant topics. These discussions are the foundations for the findings of the study.

4.2.1 Questionnaire design

In designing a questionnaire, there are many choices to be made, and factors to take into account. The literature presents several challenges for the development of questionnaires, some of which will be covered here.

Medium The first decision that had to be made was the medium of the questionnaire. The two main methods considered was a paper survey sent to the participants by mail, and an electronic survey conducted over the internet. As the expected number of respondents was low, about 10-20, there would not be an excessive amount of work, or a high cost, in sending out and processing paper surveys. The main benefit of doing a paper survey would be that it is considered truly anonymous by The Norwegian Data Protection Authority, something that eases the burden of ensuring anonymity. An electronic survey has the advantages that it can automatically calculate averages, return comparisons, and supports complex skip patterns. As there would be a need especially for skip patterns, an online survey was chosen. The anonymity implications of using an online survey are discussed later in this section.

Wording A lot of time was used deciding on the exact wording of the questions and alternatives in the questionnaire. When the questionnaire was sent out, there would be no opportunity to make clarifications or alter the survey, and getting enough data from the survey was vital to be able to conduct the interviews in an efficient manner.

[27] talks about the ambiguity of different words, and making sure that the questions are clearly understandable, while not becoming too broad. An example used is the question *"Should all physical punishment of children by parents be made illegal?"*. Problems with this formulation include the definition of "physical punishment" and "illegal", which may differ between participants of the study. A revised version that reads *"Should parents be allowed to smack their children"?* deals with these problems, but also makes the question problematically detailed. Now, only one form of physical punishment is considered, and there will be a need for more questions concerning other forms of punishment.[27]

Taking the theory of ambiguity into account, some of the more complex parts of the questionnaire were broken down into several simpler questions.

Length When presented with a survey, the length of the survey can be a deterrent to participation. The expected length of the survey is found to give a negative correlation between the number of participants starting the survey, and the number completing it [28]. Limiting the size of the survey was therefore an important goal, to ensure that there would not be any unnecessary loss of participants. Deciding on a questionnaire length was also linked to the length of the interviews. It seemed fitting to ask participants for no more than one hour of their time in total, and the interviews themselves should not last more than 45 minutes, as will be discussed in Section 4.3.1.

Based on these factors, a goal of 15 minutes was set for the completion time of the questionnaire. As estimating the time needed to answer a questionnaire is difficult, and knowing that the participants' time is valuable, erring on the side of caution was preferred when estimating the length of the survey.

Scales Several questions asked in the survey required the respondents to answer on a scale. There has been done an extensive amount of research on the subject of scales in surveys, and a review of this research suggests that a 7-point scale is optimal for surveys where the respondents themselves read the survey [29]. In the case of this survey, with the limited number of respondents and the fact that all participants would be followed up in an interview, the decision was made to use a standard 5-point Likert scale, illustrated in Figure 4.2. It was desirable to keep the option to answer neutrally (having an option with equal distance to each extreme), while not giving too many granular options, as this would make the follow-up work more difficult. Using a 5-point Likert scale also made the naming of the points easy and recognisable for the participants, with the points being named as shown in Figure 4.2.

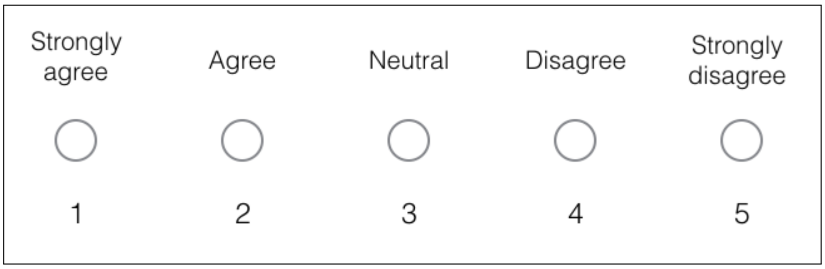


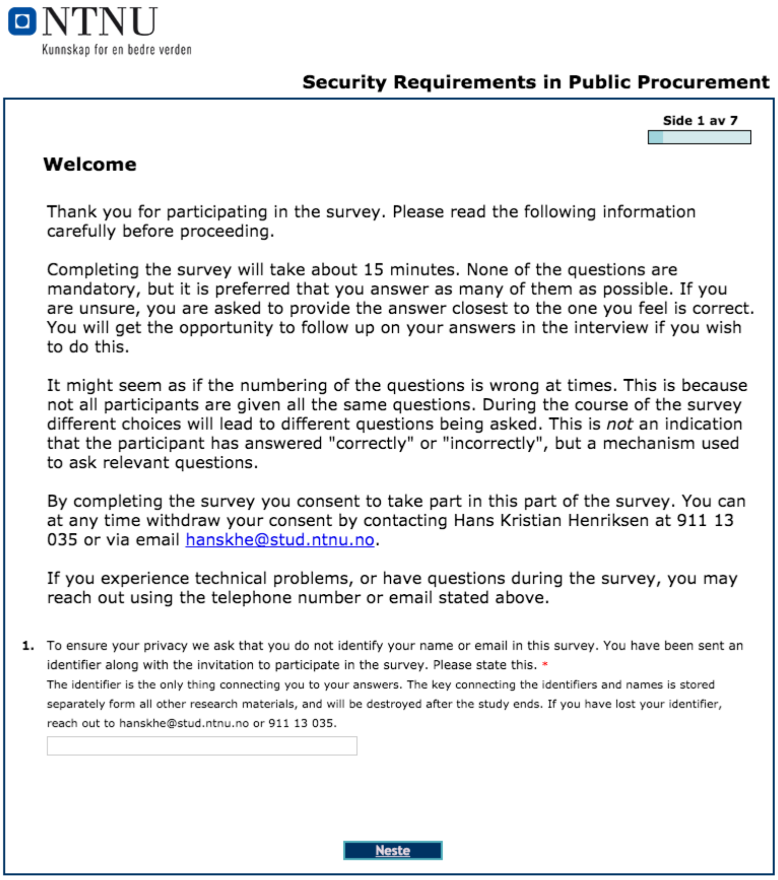
Figure 4.2: The 5-point Likert scale used in the survey

Anonymity As the topic of information security can be viewed as sensitive by some, ensuring the anonymity of the participants was vital. This was underscored by the fact that participants would be asked questions about how they feel their own organisation handles information security. Anonymity is mainly ensured in two ways. Firstly by giving the participants a unique and randomly generated identifier[1] to ensure that the answers from the survey were not linked directly to them. Secondly, the survey tool used was SelectSurvey hosted locally at NTNU by the Faculty of Social Sciences and Technology Management (SVT). This ensured that the IP-address of the respondents, which it was impossible to avoid detecting, was not sent to any third parties.

While these measures provide the respondents with the best anonymity possible, it was just as important that the respondents *felt* anonymous while completing the survey. This was accomplished by making sure the survey was perceived as trustworthy and professional. The standard NTNU layout was used, making the survey recognisable for anyone who has participated in an NTNU survey before. Information about privacy was given both on the first page of the survey and in the email containing information about the survey. The first page of the survey can be seen in Figure 4.3.

Question order Choosing the proper order for the questions can affect the outcome of the survey, both because of participant motivation, and because

[1] The identifiers were generated using www.random.org, which uses atmospheric noise to generate randomness.



Security Requirements in Public Procurement

Welcome

Thank you for participating in the survey. Please read the following information carefully before proceeding.

Completing the survey will take about 15 minutes. None of the questions are mandatory, but it is preferred that you answer as many of them as possible. If you are unsure, you are asked to provide the answer closest to the one you feel is correct. You will get the opportunity to follow up on your answers in the interview if you wish to do this.

It might seem as if the numbering of the questions is wrong at times. This is because not all participants are given all the same questions. During the course of the survey different choices will lead to different questions being asked. This is *not* an indication that the participant has answered "correctly" or "incorrectly", but a mechanism used to ask relevant questions.

By completing the survey you consent to take part in this part of the survey. You can at any time withdraw your consent by contacting Hans Kristian Henriksen at 911 13 035 or via email hanskhe@stud.ntnu.no.

If you experience technical problems, or have questions during the survey, you may reach out using the telephone number or email stated above.

1. To ensure your privacy we ask that you do not identify your name or email in this survey. You have been sent an identifier along with the invitation to participate in the survey. Please state this. *
The identifier is the only thing connecting you to your answers. The key connecting the identifiers and names is stored separately form all other research materials, and will be destroyed after the study ends. If you have lost your identifier, reach out to hanskhe@stud.ntnu.no or 911 13 035.

Figure 4.3: The landing page of the survey

providing an answer in one question might change how the participant interprets the next. It is recommended that the first questions in the survey are easy and interesting, with the questions in the middle being more difficult, and ending with some interesting questions in order to increase the likelihood of completion. [27]

This advice was followed in the setup of the questionnaire, as described in Section 4.2.2.

4.2.2 Questionnaire setup

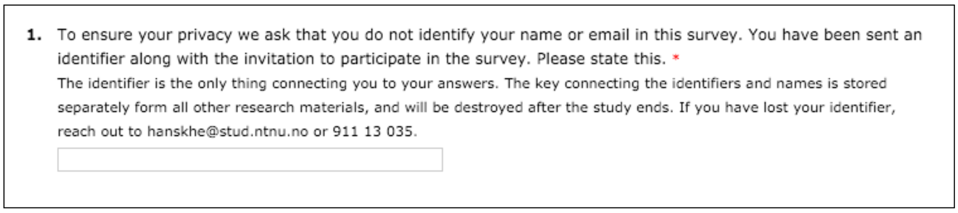
This section describes the survey that was sent to the respondents, and how the theory from Section 4.2.1 was used to ensure a survey of high quality that facilitates high response rates and accurate results.

The goal of the survey was to collect information about the participants' views in order to facilitate the interviews. One of the focus areas was to get the participants' opinions on the findings of the prestudy, in particular the seven areas of literature recommendations presented in Section 3.3.2.2, and the importance of the categories identified in Section 3.3.1.8. In addition, their opinions and attitudes towards information security, and the current state of practice in the field was of interest.

All screen shots presented in this section are a translated version of the final survey sent to the participants. The original Norwegian version is presented in Appendix A.

The survey was divided into seven sections. First, an introduction about the survey was given, and the participants were asked to provide their identifier. Following were sections with questions about basic information on the participants, security requirements in general, the participants' own security work, evaluation of security requirements, and categories of security requirements. Finally, closing information was given before the participants submitted the survey.

Introduction The participants were greeted by the introduction shown in Figure 4.3. The introduction was designed to inform the participants of the expected time to complete the survey, and give some basic instructions. As the survey tool numbers each question based on the *total* number of questions, not the *actual* number of questions shown to the participants, an explanation of this was added. The participants were informed that completing the survey constitutes consent to participation, and given contact information to the responsible for the survey.

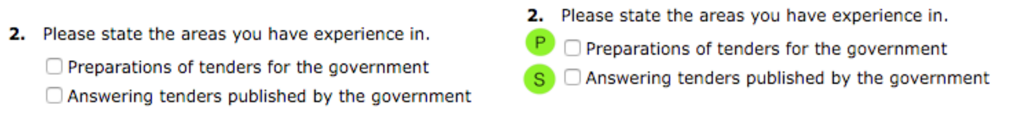


1. To ensure your privacy we ask that you do not identify your name or email in this survey. You have been sent an identifier along with the invitation to participate in the survey. Please state this. *

The identifier is the only thing connecting you to your answers. The key connecting the identifiers and names is stored separately form all other research materials, and will be destroyed after the study ends. If you have lost your identifier, reach out to hanskhe@stud.ntnu.no or 911 13 035.

Figure 4.4: Question 1: Identifier

Figure 4.4 shows the first question of the survey, asking the participants to enter their anonymous identifier. This question was mandatory, as no participant should conduct the survey without there being a way to connect their answer to them for interview preparations. In order to make the survey more trustworthy, and to relax any concerns about privacy, the identifier and how it protects the privacy of the participants, was explained.



2. Please state the areas you have experience in.

□ Preparations of tenders for the government

□ Answering tenders published by the government

(a) As presented to participants

2. Please state the areas you have experience in.

P □ Preparations of tenders for the government

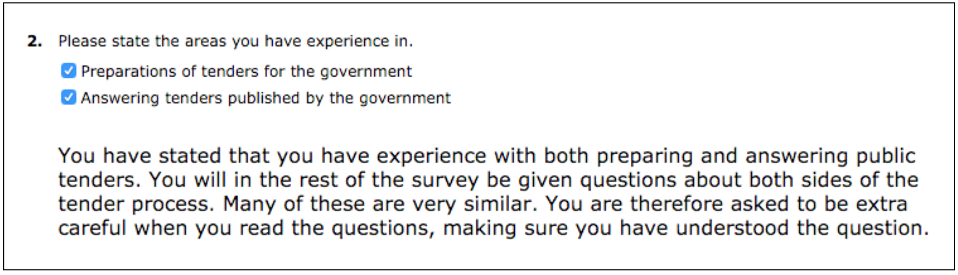
S □ Answering tenders published by the government

(b) Illustration of conditional rules activated by the participants' choice

Figure 4.5: Question 2: Field of experience

Basic information The first question in this section is shown in Figure 4.5a, and determines which questions will be asked later in the survey. Placing this question first makes it possible to remove as many irrelevant questions as possible. It is also an easy question, falling in line with the theory of not asking difficult questions early in the survey.

As illustrated in Figure 4.5b, the different choices in this question affects later questions. In the rest of the description of the survey, the marker P will be used to illustrate questions asked to participants who have indicated experience with preparation of tenders (procurers), and likewise S for those with experience with answering tenders (suppliers). Questions with no marker are presented to all participants.



2. Please state the areas you have experience in.

☑ Preparations of tenders for the government

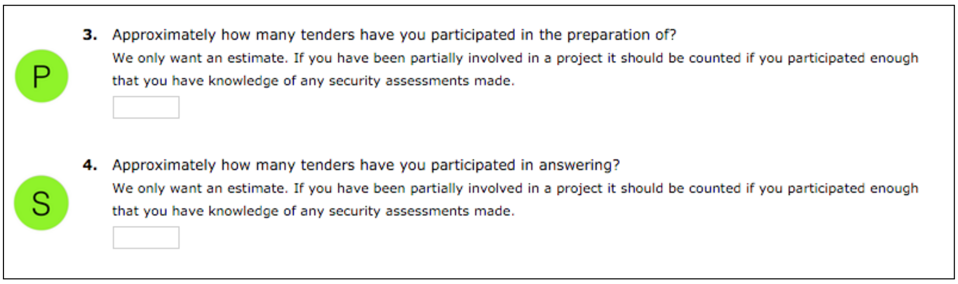
☑ Answering tenders published by the government

You have stated that you have experience with both preparing and answering public tenders. You will in the rest of the survey be given questions about both sides of the tender process. Many of these are very similar. You are therefore asked to be extra careful when you read the questions, making sure you have understood the question.

Figure 4.6: Warning displayed for participants with experience as both suppliers and procurers.

If a participant reported experience in both the fields of procuring and supplying, a warning message as shown in Figure 4.6 was displayed. This was done because the wording of many of the questions given to procurers and suppliers were very similar, and there was a real risk of these participants confusing the questions with each other.

To get an idea of how experienced the participants of the study were with tenders, they were asked to provide an estimate on how many tenders they had worked on, as shown in Figure 4.7.



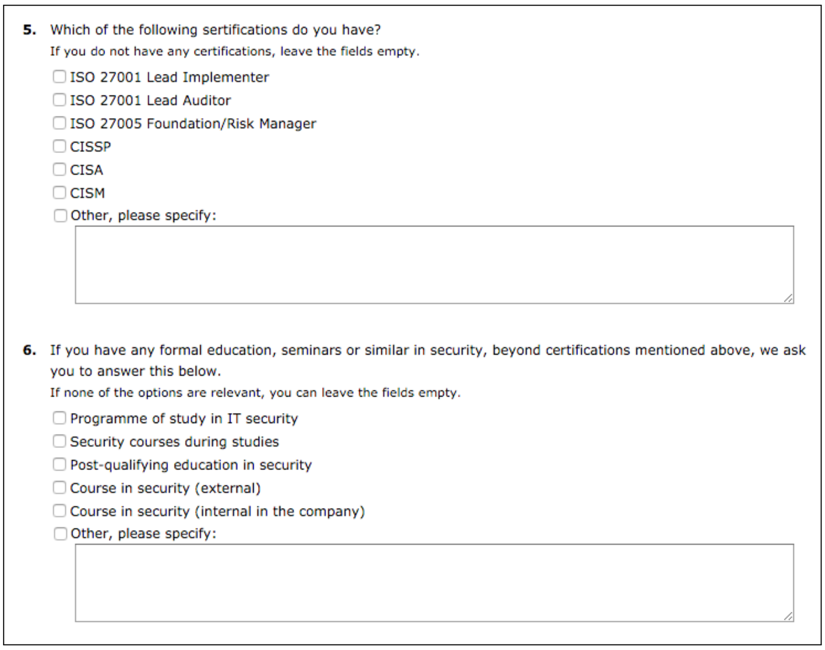
P

3. Approximately how many tenders have you participated in the preparation of?
We only want an estimate. If you have been partially involved in a project it should be counted if you participated enough that you have knowledge of any security assessments made.

S

4. Approximately how many tenders have you participated in answering?
We only want an estimate. If you have been partially involved in a project it should be counted if you participated enough that you have knowledge of any security assessments made.

Figure 4.7: Question 3 and 4: Number of tenders worked on



5. Which of the following sertifications do you have?
If you do not have any certifications, leave the fields empty.

- □ ISO 27001 Lead Implementer
- □ ISO 27001 Lead Auditor
- □ ISO 27005 Foundation/Risk Manager
- □ CISSP
- □ CISA
- □ CISM
- □ Other, please specify:

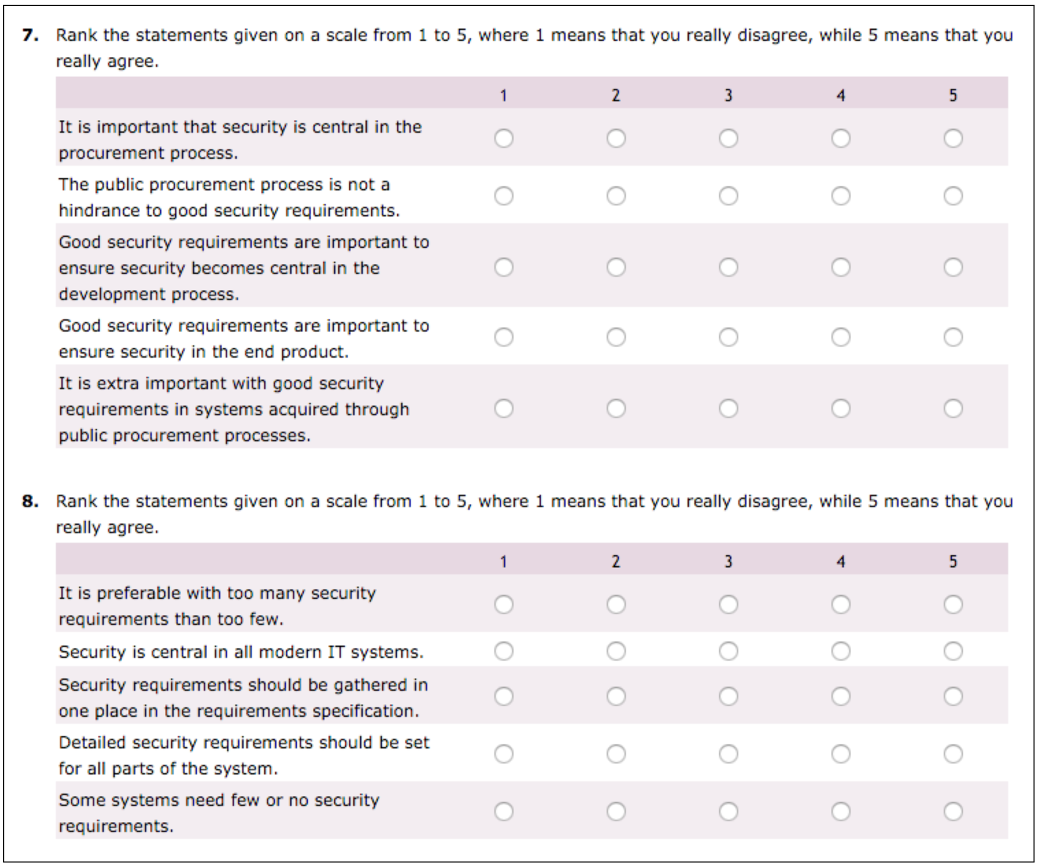
6. If you have any formal education, seminars or similar in security, beyond certifications mentioned above, we ask you to answer this below.
If none of the options are relevant, you can leave the fields empty.

- □ Programme of study in IT security
- □ Security courses during studies
- □ Post-qualifying education in security
- □ Course in security (external)
- □ Course in security (internal in the company)
- □ Other, please specify:

Figure 4.8: Question 5 and 6: Certifications and education

As part of understanding the participants, they were also asked to provide some insight into their formal education and certifications in IT security. This was done to make it possible to understand what kind of participants had been recruited, and what background they had when evaluating their answers. Figure 4.8 shows the question, and the suggested certifications and educations a participant might have. In addition, a text field was provided for participants to fill in any complementing information.

General about security requirements This section of the survey presented the participants with 10 statements divided into two blocks. The statements were to be answered on a 5-point Likert scale, as described in Section 4.2.1.



7. Rank the statements given on a scale from 1 to 5, where 1 means that you really disagree, while 5 means that you really agree.

	1	2	3	4	5
It is important that security is central in the procurement process.	○	○	○	○	○
The public procurement process is not a hindrance to good security requirements.	○	○	○	○	○
Good security requirements are important to ensure security becomes central in the development process.	○	○	○	○	○
Good security requirements are important to ensure security in the end product.	○	○	○	○	○
It is extra important with good security requirements in systems acquired through public procurement processes.	○	○	○	○	○

8. Rank the statements given on a scale from 1 to 5, where 1 means that you really disagree, while 5 means that you really agree.

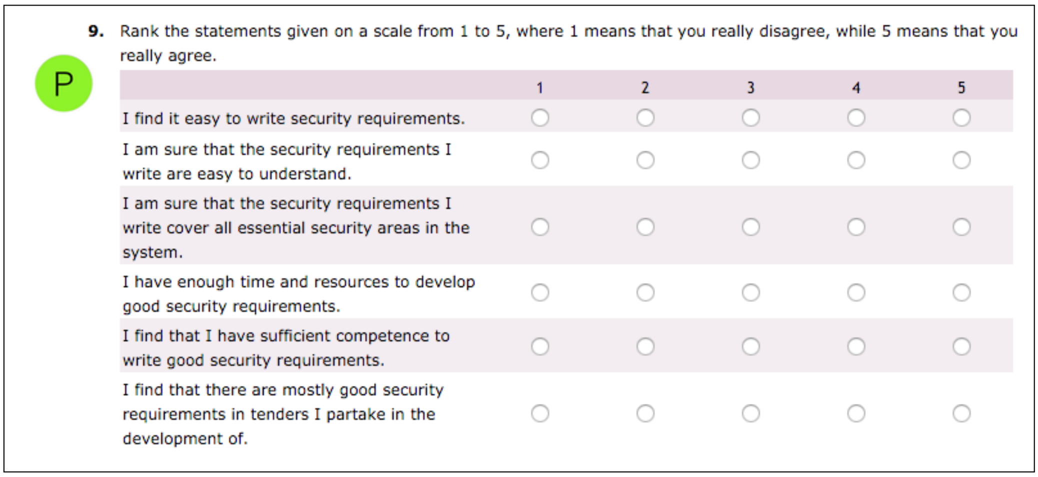
	1	2	3	4	5
It is preferable with too many security requirements than too few.	○	○	○	○	○
Security is central in all modern IT systems.	○	○	○	○	○
Security requirements should be gathered in one place in the requirements specification.	○	○	○	○	○
Detailed security requirements should be set for all parts of the system.	○	○	○	○	○
Some systems need few or no security requirements.	○	○	○	○	○

Figure 4.9: Question 7 and 8: General statements on security requirements

Figure 4.9 shows the questions asked in this part of the survey. The statements in question 7 were designed to understand the participant's attitudes on security requirements, and their use in public procurements. In question 8, some of the statements refer to the findings of the prestudy, such as the questions on gathering security requirements, and the number of security requirements. This was intended for use in the follow-up during the interviews to get a better understanding of why there might be contradictory views on the subject, as evident by the discrepancy between theory and practice found in the prestudy.

As the prestudy found several systems with no, or few, security requirements, a set of questions about this were asked. These questions were worded differently to attempt to find reasons for security requirements not being viewed as important. One possibility might be that certain types of systems are considered not in need of security requirements, or there might be a view that there are parts of systems that don't need detailed security requirements.

Participant's own work on security requirements In this section, the participants were given questions on their own work with security requirements. This was probably some of the more difficult questions in the survey, as a lot of introspection was required, and the questions were thus placed in the middle of the survey, as discussed in Section 4.2.1.



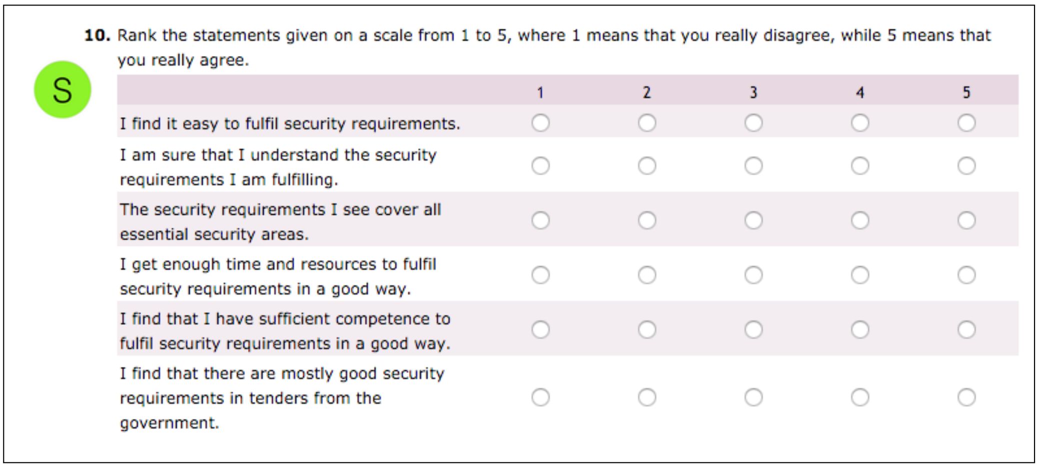
9. Rank the statements given on a scale from 1 to 5, where 1 means that you really disagree, while 5 means that you really agree.

	1	2	3	4	5
I find it easy to write security requirements.	○	○	○	○	○
I am sure that the security requirements I write are easy to understand.	○	○	○	○	○
I am sure that the security requirements I write cover all essential security areas in the system.	○	○	○	○	○
I have enough time and resources to develop good security requirements.	○	○	○	○	○
I find that I have sufficient competence to write good security requirements.	○	○	○	○	○
I find that there are mostly good security requirements in tenders I partake in the development of.	○	○	○	○	○

Figure 4.10: Question 9: Procurer's perspective on their own work with security requirements

Procurers, who write the requirement specifications, were asked about their opinions on their own work in developing security requirements. The prestudy found that a lot of the requirement documents studied were lacking in security requirements. The first three questions seen in Figure 4.10

were designed to get an understanding of the participants' view of their own work. If the procurers, in general, are of the opinion that their work is good, but this is disputed by the suppliers, that would indicate a large discrepancy between the purchasers' and suppliers' understanding of security requirements. Following were two questions designed to understand if the purchasers themselves find that their time, resources and competence is sufficient. The findings in the prestudy could be explained by the procurers not having the necessary resources or competence to develop high-quality security requirements. Finally, the participants were asked to evaluate the overall security requirements in tenders they partake in.



10. Rank the statements given on a scale from 1 to 5, where 1 means that you really disagree, while 5 means that you really agree.

	1	2	3	4	5
I find it easy to fulfil security requirements.	○	○	○	○	○
I am sure that I understand the security requirements I am fulfilling.	○	○	○	○	○
The security requirements I see cover all essential security areas.	○	○	○	○	○
I get enough time and resources to fulfil security requirements in a good way.	○	○	○	○	○
I find that I have sufficient competence to fulfil security requirements in a good way.	○	○	○	○	○
I find that there are mostly good security requirements in tenders from the government.	○	○	○	○	○

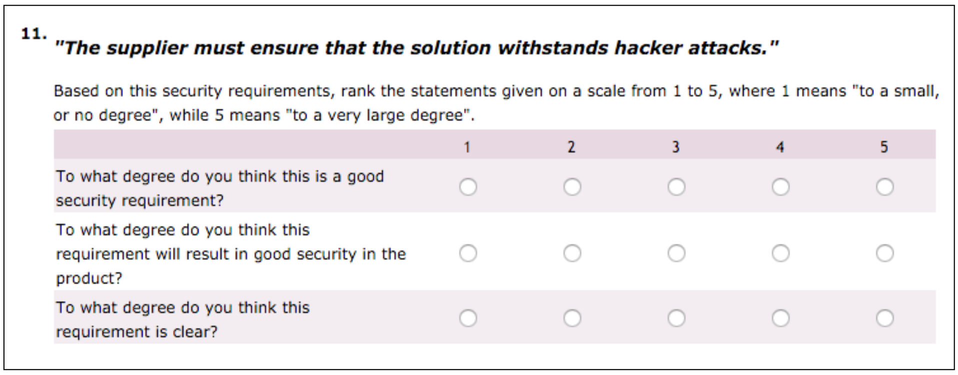
Figure 4.11: Question 10: Supplier's perspective on their own work with security requirements

Figure 4.11 presents the questions on the topic asked to suppliers. They are very similar, though seen from the opposite viewpoint, to the questions in Figure 4.10. The only major difference is the last question, where procurers were asked about the general quality of requirements in tenders they themselves partake in. Participating suppliers were here asked about the quality of security requirements from the government in general, as they were expected to have worked with numerous governmental tenders.

The questions in this section of the survey were quite personal, and touched on the participants' own competence and their organisation's ability to efficiently prevent security issues. This was thus an area where there was a possibility that the participants would not answer accurately. Steps taken to reduce the risk was the overall trustworthiness of the survey, placing the questions in the middle of the survey to allow a rapport to be built with the participant before they reach these questions, and giving the questions a positive spin.

Evaluation of security requirements To gain a better understanding of the attitudes towards certain security requirements, the participants were asked in this section to rate several security requirements on three different merits. The first merit was whether the security requirement itself was good. This was followed by whether the requirement would ensure good security, and finally, if the requirement was clear. Splitting the evaluation in three parts allowed the participants to more granularly rate the requirements, without having to decide which of the three factors was most important. One could imagine a requirement that was considered good on a theoretical level, but that the participant understood would perform badly in the real world, and this was something that was desirable to investigate.

The security requirements in this section of the questionnaire were designed to have one or more flaws in accordance with the conclusions of the prestudy [1]. The goal was to see if these flaws were identified by the participants and if they were viewed as problematic. As such, none of the requirements presented here were made to be of high quality, but rather to have engineered flaws to facilitate a discussion with the participants. All the requirements in this section were presented to all participants in the survey.



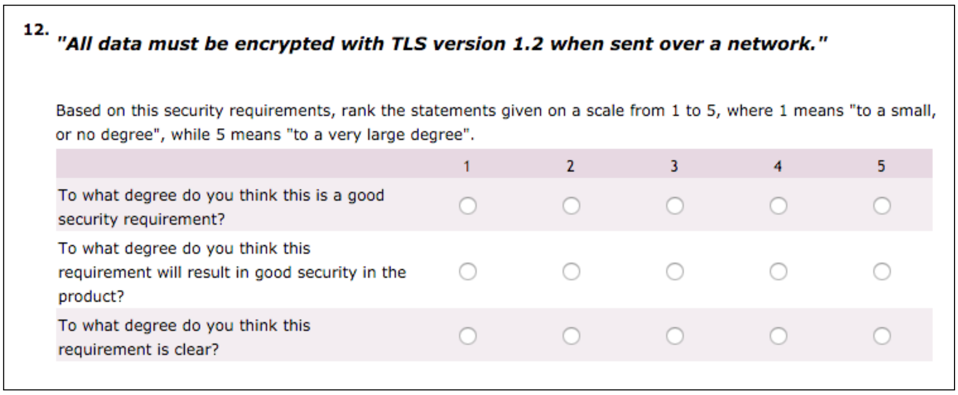
11. ***"The supplier must ensure that the solution withstands hacker attacks."***

Based on this security requirements, rank the statements given on a scale from 1 to 5, where 1 means "to a small, or no degree", while 5 means "to a very large degree".

	1	2	3	4	5
To what degree do you think this is a good security requirement?	○	○	○	○	○
To what degree do you think this requirement will result in good security in the product?	○	○	○	○	○
To what degree do you think this requirement is clear?	○	○	○	○	○

Figure 4.12: Question 11: Blanket statement on hacker security

Question 11, as seen in Figure 4.12, presents a requirement asking the supplier to ensure that the system being developed can withstand hacker attacks. The requirement was written to be extremely broad, modelled on requirements found in the prestudy that basically put the entire responsibility of a hacker attack on the supplier. The goal of asking this question was to get an understanding of why a procurer might include such a requirement, and how a supplier would react if presented with it.



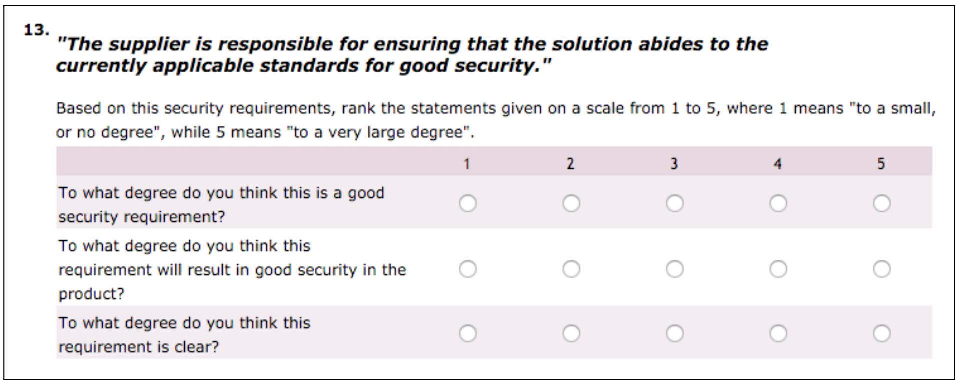
12. ***"All data must be encrypted with TLS version 1.2 when sent over a network."***

Based on this security requirements, rank the statements given on a scale from 1 to 5, where 1 means "to a small, or no degree", while 5 means "to a very large degree".

	1	2	3	4	5
To what degree do you think this is a good security requirement?	○	○	○	○	○
To what degree do you think this requirement will result in good security in the product?	○	○	○	○	○
To what degree do you think this requirement is clear?	○	○	○	○	○

Figure 4.13: Question 12: Requirement with very specific version of TLS

With question 12 (Figure 4.13), the goal was to investigate the effect of a very specific choice of technology. The theory suggests that this would be an unnecessary constraint on the system, and that there is a risk that the technology choice is outdated when the system is complete. The question was meant as the basis for a discussion on the potential problems of over-specifying security requirements, and making choices about specific technologies.



13. ***"The supplier is responsible for ensuring that the solution abides to the currently applicable standards for good security."***

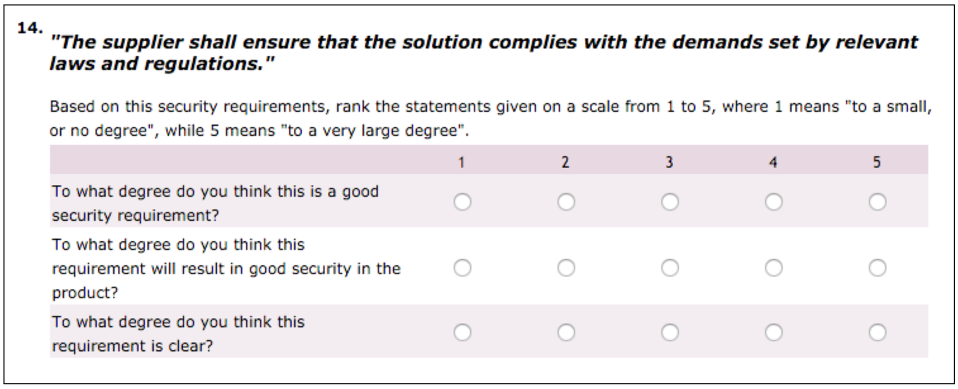
Based on this security requirements, rank the statements given on a scale from 1 to 5, where 1 means "to a small, or no degree", while 5 means "to a very large degree".

	1	2	3	4	5
To what degree do you think this is a good security requirement?	○	○	○	○	○
To what degree do you think this requirement will result in good security in the product?	○	○	○	○	○
To what degree do you think this requirement is clear?	○	○	○	○	○

Figure 4.14: Question 13: Broad statement on current standards for good security

Question 13, as seen in Figure 4.14, investigated attitudes towards requirements that have broad or vague statements on ”current standards”.

The prestudy found several instances of requirements that asked the supplier to confirm that they followed ”best practice”, without specifying this, or with very broad definitions. The goal of this question was to get input on whether these kinds of requirements could have a positive effect on the final product, or if they were primarily used as a tool to make the supplier accept all responsibility for security related issues.



14. ***"The supplier shall ensure that the solution complies with the demands set by relevant laws and regulations."***

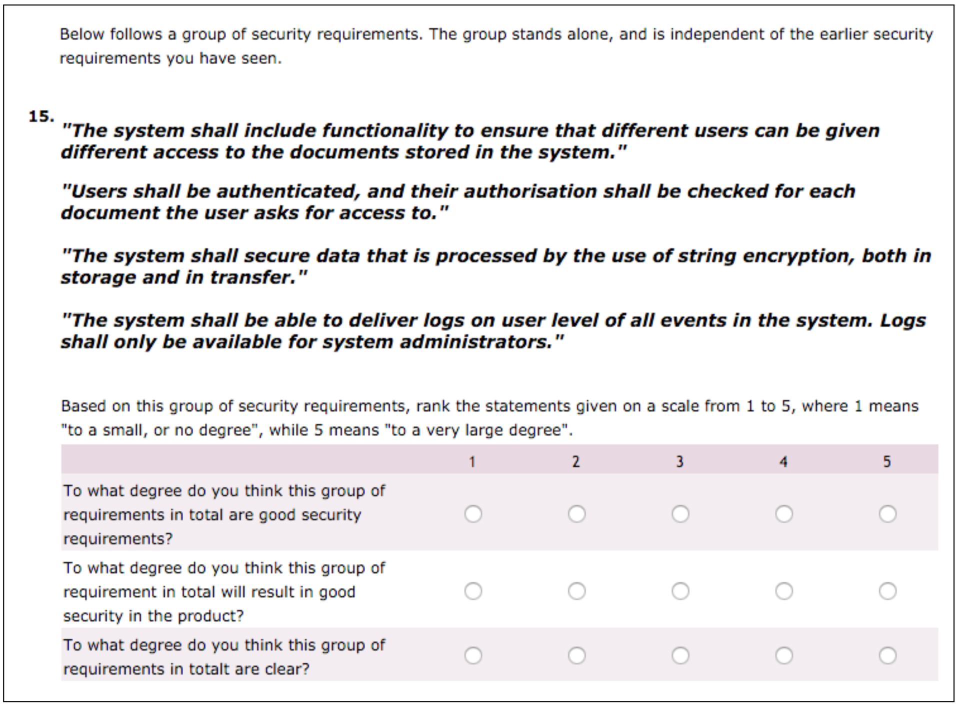
Based on this security requirements, rank the statements given on a scale from 1 to 5, where 1 means "to a small, or no degree", while 5 means "to a very large degree".

	1	2	3	4	5
To what degree do you think this is a good security requirement?	○	○	○	○	○
To what degree do you think this requirement will result in good security in the product?	○	○	○	○	○
To what degree do you think this requirement is clear?	○	○	○	○	○

Figure 4.15: Question 14: Broad statement on relevant laws and regulations

Question 14 (Figure 4.15) is in many ways quite similar to question 13. They both pertain to broad statements on what must be covered by the supplier. In question 14 the subject is laws and regulations, and the requirement makes it the suppliers' responsibility that they are followed. Further, the requirement also leaves it to the suppliers to identify relevant laws and regulations. The results from this question could be used for discussion on whether relevant laws and regulations should be specified by the purchaser.

In the questions leading up to question 15, the participants have been asked to provide their position on single requirements. It is, however, important to see security requirements as a collection of several requirements interacting with each other. As seen in Figure 4.16, a set of four security requirements were presented to the participants. The group of requirements was constructed based on a fictional system that contained sensitive data. The areas of encryption, authentication, authorisation and logging have been covered by the requirements. However, requirements regarding physical security, incident management, and compliance have been left out. The goal was to see if the participants view the set of requirements as good, or if they would have input on the missing areas.



Below follows a group of security requirements. The group stands alone, and is independent of the earlier security requirements you have seen.

15. ***"The system shall include functionality to ensure that different users can be given different access to the documents stored in the system."***

"Users shall be authenticated, and their authorisation shall be checked for each document the user asks for access to."

"The system shall secure data that is processed by the use of string encryption, both in storage and in transfer."

"The system shall be able to deliver logs on user level of all events in the system. Logs shall only be available for system administrators."

Based on this group of security requirements, rank the statements given on a scale from 1 to 5, where 1 means "to a small, or no degree", while 5 means "to a very large degree".

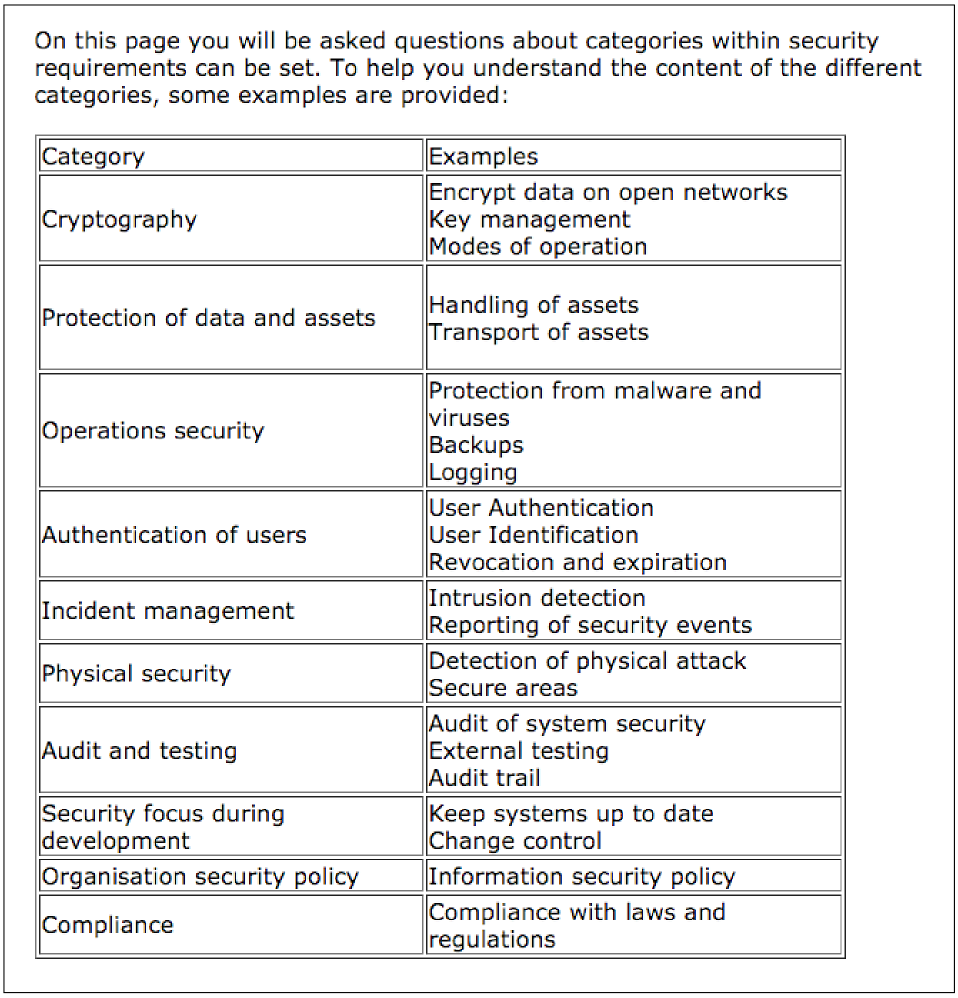
	1	2	3	4	5
To what degree do you think this group of requirements in total are good security requirements?	○	○	○	○	○
To what degree do you think this group of requirement in total will result in good security in the product?	○	○	○	○	○
To what degree do you think this group of requirements in totalt are clear?	○	○	○	○	○

Figure 4.16: Question 15: Group of requirements to examine inconsistency in requirement selection

Security requirement categories In the prestudy, 10 categories of security requirements were identified, based on ISO 27002, Common Criteria and PCI-DSS. The goal was to be able to better categorise security requirements, and provide a basis for work on security requirements. This is further discussed in Section 3.3.1.8.

In this section of the survey, the participants were presented with a condensed explanation of the security categories, as shown in Figure 4.17. Based on this information, questions 16 to 18 asked participants to report their position on the importance and use of requirements in these categories.

It was interesting to get a sense of the priorities the participants would have, if made to rank the categories on importance. They would obviously have different interpretations of the categories, and place them into different contexts, but the results would facilitate the start of a conversation. It was also interesting to see if any areas were evaluated especially high or low, or if there were other patterns emerging. Question 16 (Figure 4.18) asks the participants to rank the categories using numbers from 1 to 10, with 1 being the highest ranked, and thus the most important category.

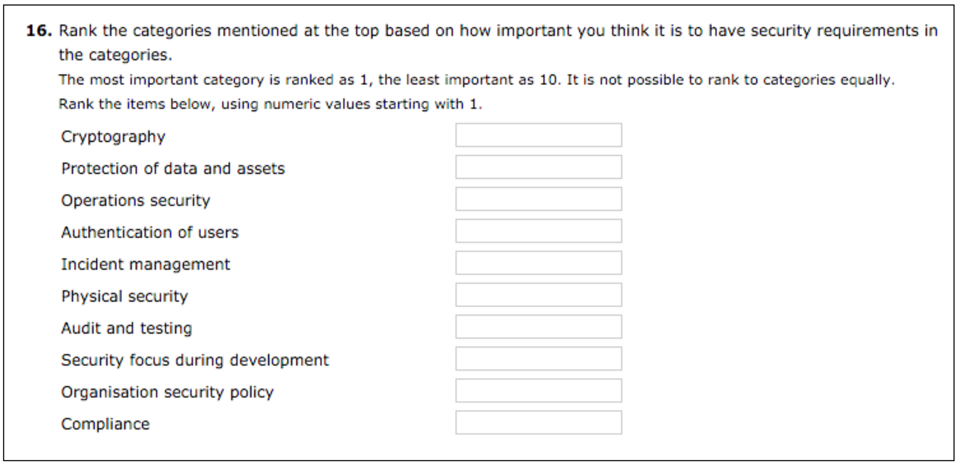


On this page you will be asked questions about categories within security requirements can be set. To help you understand the content of the different categories, some examples are provided:

Category	Examples
Cryptography	Encrypt data on open networks Key management Modes of operation
Protection of data and assets	Handling of assets Transport of assets
Operations security	Protection from malware and viruses Backups Logging
Authentication of users	User Authentication User Identification Revocation and expiration
Incident management	Intrusion detection Reporting of security events
Physical security	Detection of physical attack Secure areas
Audit and testing	Audit of system security External testing Audit trail
Security focus during development	Keep systems up to date Change control
Organisation security policy	Information security policy
Compliance	Compliance with laws and regulations

Figure 4.17: The ten categories of security requirements, as identified in [1]

While it was interesting to know how important the participants viewed the different categories, the real state of practice was also important. In questions 17 and 18 the participants were asked to select the three most common categories for them to either write requirements for (Figure 4.19), or to see requirements written for (Figure 4.20). Combining the results from question 16 and 17/18 could prove interesting, especially if the case was that the categories that were viewed as most important were not the same as the ones most often used in requirements. The answers to questions 17 and 18 would, of course, be subjective, and based on the memory and intuition of the participants. However, as the participants were expected to be experienced security operatives, they would likely already have an idea of the most



16. Rank the categories mentioned at the top based on how important you think it is to have security requirements in the categories.

The most important category is ranked as 1, the least important as 10. It is not possible to rank to categories equally.

Rank the items below, using numeric values starting with 1.

Cryptography

Protection of data and assets

Operations security

Authentication of users

Incident management

Physical security

Audit and testing

Security focus during development

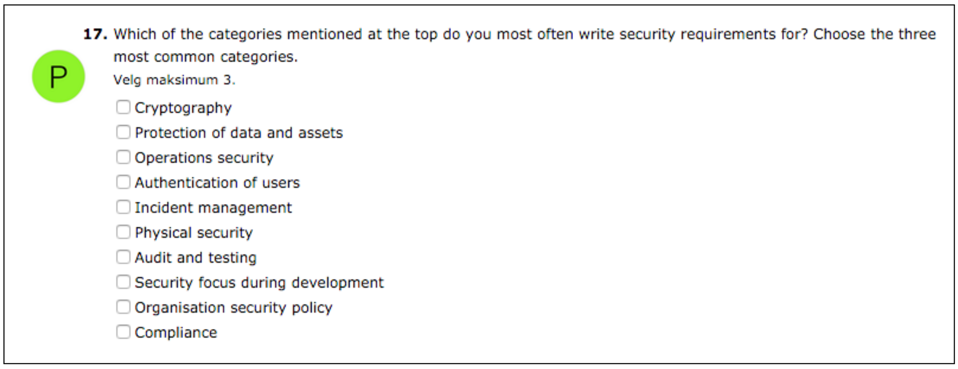
Organisation security policy

Compliance

Figure 4.18: Question 16: Ranking of the ten categories based on their importance

common areas of requirements before taking part in the survey.

Closing information After answering all the questions of the survey, the participants were shown the closing information seen in Figure 4.21. Participants were informed that their completion of the survey would be regarded as consent for participation, and were given contact information for the author, should they like to withdraw, or have questions.

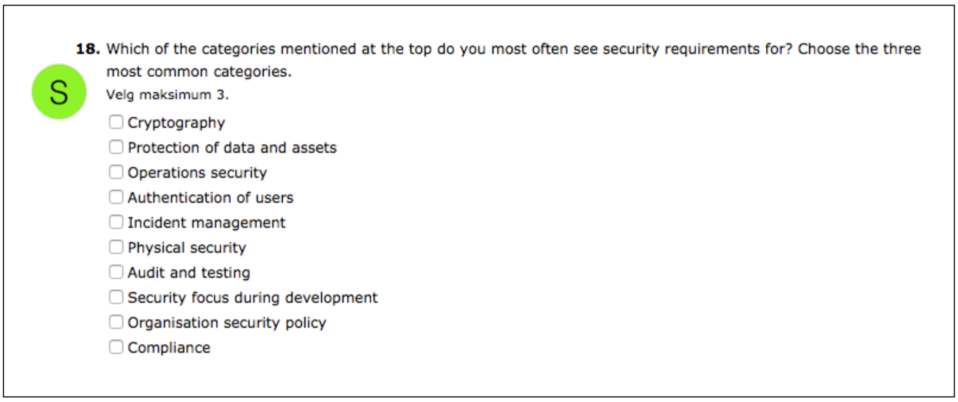


17. Which of the categories mentioned at the top do you most often write security requirements for? Choose the three most common categories.

Velg maksimum 3.

□ Cryptography
□ Protection of data and assets
□ Operations security
□ Authentication of users
□ Incident management
□ Physical security
□ Audit and testing
□ Security focus during development
□ Organisation security policy
□ Compliance

Figure 4.19: Question 17: Selection of the three categories security requirements are most commonly written for

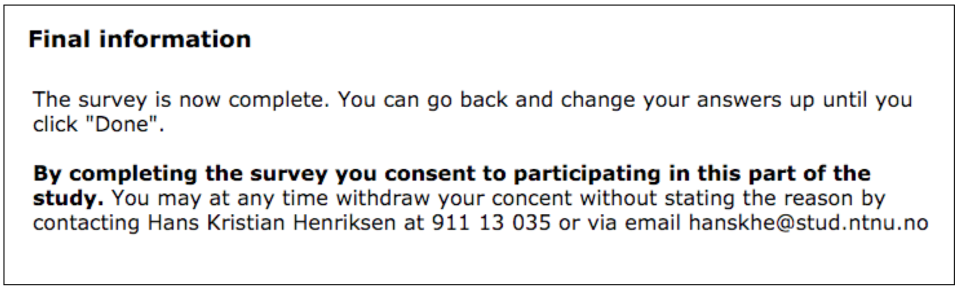


18. Which of the categories mentioned at the top do you most often see security requirements for? Choose the three most common categories.

Velg maksimum 3.

□ Cryptography
□ Protection of data and assets
□ Operations security
□ Authentication of users
□ Incident management
□ Physical security
□ Audit and testing
□ Security focus during development
□ Organisation security policy
□ Compliance

Figure 4.20: Question 18: Selection of the three categories for which security requirements are most commonly seen



Final information

The survey is now complete. You can go back and change your answers up until you click "Done".

By completing the survey you consent to participating in this part of the study. You may at any time withdraw your concent without stating the reason by contacting Hans Kristian Henriksen at 911 13 035 or via email hanskhe@stud.ntnu.no

Figure 4.21: Closing information given before the survey is submitted

4.2.3 Questionnaire testing

Testing the questionnaire before it is sent to the participants is important, both to ensure that the survey is technically functioning, and to get feedback on the wording of questions, time used, and the overall experience of the survey [27, 29]. One recommendation is to first conduct an informal test with friends family and colleagues, before running a test with participants in the target audience [27].

As there was no abundance of people in the target audience, this turned out to be difficult. It would be problematic to ask the already recruited participants to be part of the test group, as this was a task they had not signed up for, and there was a possibility that this would prime them, or change their answers when they received the questionnaire the second time. Due to this, and to time constraints, it was decided to only run informal tests of the wording and technical functionality of the survey. The tests were conducted on a live version of the survey, to ensure that the testers experienced the exact survey the participants would see. Lillian Røstad was asked to go through the survey, as she has good knowledge of the subject matter, and would be able to identify weaknesses only a person with domain knowledge could. In addition, a few fellow students were asked to review parts of the survey and the wording of specific questions that were difficult to formulate satisfactorily.

Changes based on feedback Two main changes were made to the questionnaire due to the feedback from the testers.

The survey tool used, SelectSurvey, has functionality built in to validate answers against a set of rules. As there were some fields where the users could input any value, it was thought to be a good idea to implement some simple validation of these fields. The questions about the number of tenders the participant has been involved in, as shown in Figure 4.7, was set to validate that a number greater than or equal to 0 was entered. As these fields were shown to the users conditionally, based on their choice in question 2 (Figure 4.5a), most participants would only be shown one of these input fields. Due to a bug in the survey tool, fields that are not displayed to the user are still validated, and since the user has no way of entering a value into a hidden field, this produced an error the user could not correct.

Adding to the problem, while the question is not marked as mandatory, the validation system overrides this and prevents the user from advancing in the survey if a validation error is present, causing the question to become *de facto* mandatory. This was not discovered in initial testing, as all testing included checking both checkboxes in question 2, in order to be shown all questions during testing. No way was found to bypass the bug, and the solution was then to deactivate the validation, accepting that some users might by mistake enter a value that could not be automatically processed by the survey tool. With no more than 20 participants expected, this was an acceptable risk.

In addition, several questions were revisited to be either reworded, made more precise, more readable, or it was decided that the question should be split into several questions or merged with another question. Question 5 (Figure 4.8) had some certifications removed, as they were viewed as obscure or rare. In question 7 (Figure 4.9), the statement *"The public procurement process is not a hindrance to good security requirements."* was originally worded *"The public procurement process creates few extra challenges with regards to security requirements."*. This was viewed as a difficult sentence to parse, with room for misinterpretations. The sentence could easily be read as *"The public procurement process creates* ***a*** *few extra (...)"*, dramatically altering the question. In addition, the wording was unnecessarily complex compared to the intention, which was to understand if the participants viewed the process of procurement as a problem in their work.

Feedback not resulting in changes Question 16 (Figure 4.18) asks the participants to rank the different categories of security requirements. This was done by having the participants enter the numbers from 1 to 10 into textboxes, something that was not seen as ideal. It was easy to forget which numbers had been used, and if the participants wanted to make changes after entering all 10 numbers, it might require some work on the part of the participant. This feedback was seen as relevant, but the survey tool did not support any other way of ranking different options. Getting answers to the question was interesting, both to get an overview of how the participants viewed the categories, but also as a basis for conversation in the interviews. Therefore, the question was kept and no changes were made to the way the ranking works, though the solution was not ideal.

4.2.4 Questionnaire distribution

After participants had agreed to participate in the study and an appointment had been made, a link to the questionnaire was sent through email. The email thanked the participants for volunteering their time to the survey and informed participants of the privacy considerations that had been made. The email included the randomly generated identifier described in Section 4.2.1, and explained its usage. A deadline for providing an answer to the survey was set, giving the participants around 10 days after the email was sent to complete the questionnaire. Participants were also informed about the registered time and place for the interview appointment, giving an opportunity to correct any mistakes. Attached to the email, participants were presented with the consent form required by NSD and asked to read it before the interview. The consent form is presented in Appendix C.

4.2.5 Post questionnaire work

After the participants had answered the survey, the results for each individual respondent was reviewed. The main goal of the review was to gain an understanding of the respondent and his/her attitudes towards the questions posed in the survey. With that information, preparing for the interviews could be done more easily, and going through the answers also helped prepare mentally for the interviews. The answers of the participants were also evaluated against the average answers, attempting to find participants with views that differed from the consensus of the group. Any question where the answers did not make sense or were contradictory to each other were also marked. Based on this information, the most important questions to ask each participant could be marked in the interview guide, which is described in Section 4.3.2. The questions in the interview guide, and their order, were also altered based on the answers in the survey to ensure the best possible utilisation of the participants' time.

4.3 Interviews

To get a deeper understanding of the current state of practice for procured software, it was decided to conduct a set of interviews. An interview makes it possible to get qualitative information that would have been impossible to capture through a questionnaire. Providing as much information in writing as contained in a conversation would not be feasible to ask of participants, and would likely have resulted in very few responses. Therefore, interviews were necessary to get the needed information to answer the research questions in this study.

There are in general three different types of interviews that are conducted with a single participant: *Fully structured*, *semi-structured* and *unstructured* [27].

Fully structured The interviewer has a set of predetermined questions, and usually asks these in order with no room for improvisation or follow-up [27, 30].

Semi-structured The interviewer has a subject for discussion, and may have some predetermined questions, in what is known as an *interview guide*. The wording of the questions can be varied, not all must be used, and based on the discussion other themes may become the topic of the interview. [27, 30]

Unstructured The interviewer has only a theme for discussion, and the participant leads the conversation [27, 30].

When employing a structured interview, the person conducting the interview does not need to have any knowledge about the subject of discussion. This is ideal when interviewing a large number of people, making it impossible for the research team to personally interview all participants. For semi-structured and unstructured interviews, the interviewer must have good knowledge of the research itself, and is usually one of the researchers themselves.[30]

This study required a more flexible way of conducting the interviews than a structured interview, as the author was not intimately familiar with the process of writing and fulfilling security requirements. Most likely, the interview subjects would present a new, unexpected, angle during the interviews, which would have been missed without the option to inquire further. By choosing a semi-structured interview, there was freedom to move into themes and discussions that could not have been foreseen as relevant by the interviewer, but that turned out to be highly interesting during the interview. At the same time, there would be some thought about how the interview was to proceed, and a clear goal with the conversation.

As described in Section 4.1, the participants were recruited from the personal network of the author and the advisers. In total, 14 people participated in the study, employed at 12 different organisations and businesses.

4.3.1 Interview guide design

The most important factor in preparing for the interviews was the creation of the interview guide. This document is the main support of the interviewer during the interviews, and contains areas of interest, sample questions and relevant prompts. In making the interview guide, there are several factors that are critical to success, the most important of which are covered below.

Question order When interviewing a stranger it is important to gain this person's trust, and be able to make the participant feel at ease [31]. This is often described as *building rapport* with the interview subject, an important skill for any interviewer [27]. For a novice interviewer, this can be a real challenge, and designing the interview guide to facilitate this process was central. If the interview subject does not trust the interviewer, it is unlikely that they will contribute with anything of great value to the study. [32] recommends some kind of "small talk" before the important questions start, and [33] suggests asking questions about the present before questions on the past or future. Consequently, the first question of the interview guide was simply: *"Can you tell me a little about your day to day work"*. This was a safe question where the participants could choose themselves what to focus on, and not something that would leave the participants thinking too much about what to answer. It also encouraged the participants to talk uninterrupted for a couple of minutes, setting the stage for the rest of the interview.

After this easy start, the questions in the interview guide followed the same pattern as the questionnaire, as this order makes it possible to collect information about the participants' attitudes on security requirements in general, before talking about how security was implemented in their organisation. Asking the questions in this order aimed to ensure that the participants were not primed to present the method used in their organisation as the best method overall.

Wording The way a question is worded can impact the answers given by the participants. Ensuring that the questions were worded optimally was important in the design of the questionnaire. The specific wording of questions for the questionnaire was discussed in Section 4.2.1. Most of this is also relevant to the wording of questions for the interview guide, but there are differences. The main difference is that the specific words used are less important for the interview guide, as the main goal is for the questions to encourage a conversation within the theme of the question [34]. In addition, as the interviews are semi-structured as mentioned in Section 4.3, the questions would not necessarily be used in the exact form they were written down in. They were provided as a starting point for a conversation on the theme, but could be altered to better fit each individual interview.

Question properties The properties of a question can also affect the answers given by participants. Especially three properties that can impact the quality of questions in interview studies were considered: open questions, leading questions and double-barreled questions.

The use of open questions is important, as it encourages the participants to not answer simply yes or no, but to talk about the topic in depth. Open questions might also make the participants anticipate follow-up questions, and answer them without having to be asked the questions, moving the conversation along. [35]

Leading questions should be avoided, though this can be difficult. The wording of the questions must be so that none of the interviewers opinions or biases are revealed to the participant, as this might change how they answer. [31] Avoiding leading questions can be especially challenging when conducting a semi-structured interview, as some questions will have to be thought of during the interview, without adequate time to consider possible ways to pose the question.

Double-barreled questions are multiple questions put together as one, e.g *"Do you think security is important, and is it more important today than before?"*. These should be avoided, as they can be difficult to answer, and might not be answered fully [36, 37]. Such questions should pose less of a problem in an interview than a questionnaire, as follow-up questions can be asked if the entire question is not answered. This can, however, elude the interviewer, and the question might be seen as complicated by the participant.

Probes and prompts When participants have answered one of the questions in the interview, there might be a need for an elaboration on the topic. Facilitating this is done through the use of probes, which are a set of questions, statements and signals that encourage the participants to keep talking, go deeper into the matter at hand, or present the reasoning behind their statements. Commonly used probes are:

Continuation probes Making the participant continue talking on the same subject, performed by e.g. saying "Mhm", or repeating the last thing the participant said.[34]

Elaboration probes Saying either *"Can you give an example?"* or *"Can you tell me more about..."?* in order to make the participant elaborate on the subject.[34]

Clarification probes Asking *"What?"* or asking the participant to provide more context for a statement, in order to clarify their opinion.[34]

Probes can also be non-verbal, using facial expressions, moving or shifting body posture, or simply remaining quiet, making the participant filling the silence [34].

While probes are general tools that can be used throughout the interview, prompts are more prepared statements or topics to bring up for each specific theme, if the participant fails to mention them [38]. A set of prompts were developed for the interview guide, and is shown in Section 4.3.2, divided between prompts that clarify the topic at hand, and prompts that move the conversation further into the topic.

Interview duration When deciding upon an interview duration, the main goal was to allot as much time as possible, while ensuring that participants would not be discouraged from participating, or become bored during the interview. A full hour seemed too long, as the prospect of talking to someone for 60 minutes appeared to be a psychological barrier. On the other hand, 30 minutes would probably not allow for more than 20 minutes of real questions, losing 5 minutes to warm-up questions, and 5 minutes to formalities such as the signing of consent forms, and answering questions about the study itself. A middle ground of 45 minutes was decided upon, with the added benefit of the total time needed from participants being 1 hour including the questionnaire. Being able to tell participants that only 1 hour in total would be needed to take part in the study was thought to help recruitment.

4.3.2 Interview guide setup

This section presents the final interview guide, and the use of the theory from Section 4.3.1. Each question has associated probes designed to make the participant either move deeper into the subject, or to expand on the topic in general. Some of the questions were asked to all the participants, while there are also different questions for the suppliers and procurers. The same notation is used here as in Section 4.2.2, with the marker P used for questions asked only to procurers, and S used for questions for the suppliers. The questions asked to all participants are unmarked.

The interview guide was developed in Norwegian, but is presented in a translated version in this chapter. The original Norwegian version is given in Appendix B.

Following the format of the questionnaire, the interview guide was divided into seven sections, and while similar to the ones for the questionnaire, there were some slight differences. First, the participants were given general information about the survey, the privacy concerns and how to withdraw from the survey. After this, a warm-up question was asked, followed by questions in general on security requirements, the participants' own security work, evaluation of requirements, general about security requirements, and closing questions. Before the interviews were ended, the participants were encouraged to talk about anything they felt had not been covered yet, and ask questions about the study.

General information Before the interviews started, the participants were informed about the background of the study, and how the data about them would be handled. Handling of the recordings done during the interviews was addressed, and the fact that no names of either the participant, nor their company would be published was emphasised. Importantly, participants were informed of their right to at any moment withdraw from the study without providing a reason, and told that they may ask that any question was skipped. Lastly, the participants were asked whether they had any questions. The notes used during this part of the interview are presented in Appendix D.

Warm-up question As described in Section 4.3.1, the goal of the first question was to make the participants comfortable with the interview situation. The question is presented in Table 4.1, and provided the participants with the opportunity to talk about the parts of their job they were comfortable discussing, without probing too far into details. If the participants were hesitant, simple prompts such as asking about their main duties, or what they find most exciting could be used.

Table 4.1: Question 1: Warm-up question

Question	**Can you tell me a little about your day to day work?**
Clarification	• What are your main duties? • Do you work a lot with teams?
Follow-up	• What takes up the most time? • What do you find most exiting?

General about security requirements The first question about security requirements pertained to the importance of the requirements given in the requirement specification, and is presented in Table 4.2. In the prestudy, many tenders had lacking security requirements in the requirement specifications, and this question was designed to investigate whether this was seen as a problem.

Questions 3 and 4, given in Tables 4.3 and 4.4, relates to the procurement process, and how this affects security requirements. Both questions were asked to all participants, though with slight modifications as indicated. The core of the questions was whether there are parts of the procurement process that makes it difficult to work with security requirements, and what can be done about this. In question 7 of the questionnaire (Figure 4.9), the participants were asked to rate a statement about this topic: *"The public procurement process is not a hindrance to good security requirements"*. Their answers were noted in the interview guide and brought up when talking about

Table 4.2: Question 2: The importance of security requirements in the tender documents

Question	**How central do you think it is for the security requirements to be finished when a tender is sent to the suppliers?**
Clarification	• A counter example would be that security requirements are not defined, but are part of the conditions of a framework agreement, or • Broad requirements: ”The customer shall ensure good security in the solution” • Why? • What is the consequence of this not being done?
Follow-up	• What do you think is the best way to solve this?

the topic in the interview, giving the participants the option to change their mind, or explain their answer in the questionnaire.

Table 4.3: Question 3: The effect of the procurement process on setting security requirements

Question	**(S: If you set yourself in the place of those writing tenders:) How do you think the procurement process influence the possibility to set good security requirements?**
Clarification	• There are some limitations in the procurement process, e.g. connected to changes, communication with suppliers and so on. Does any of these influence the possibility to set good requirements? • Are there other hindrances? • Is there anything facilitating good requirements?
Follow-up	• What is the most important change that could be made in the procurement laws to make it easier to work with security requirements?

Table 4.4: Question 4: The effect of the procurement process on fulfilling security requirements

Question	**(P: If you set yourself in the place of those answering tenders:) How do you think the procurement process influence the possibility to fulfil security requirements in a good way?**
Clarification	• There are some limitations in the procurement process, e.g. connected to changes, communication with suppliers and so on. Does any of these influence the possibility to fulfil requirements in a good way? • Are there other hindrances? • Is there anything facilitating fulfilment?
Follow-up	• What is the most important change that could be made in the procurement laws to make it easier to work with security requirements?

Question 5 (Table 4.5) was asked to procurers and concerns what is communicated in security requirements. The question was motivated by the stark differences between the security requirements found in the prestudy, and aims to understand what attributes the participants find important in the communication of security requirements. Question 6 is almost identical, but aimed at suppliers, and presented in Table 4.6.

Table 4.5: Question 5: The communication of security requirements (Procurers)

Question P	**What to you think is most important for a procurer to communicate in their security requirements?**
Clarification	• Is it concrete functions, or e.g. security goals? • Why? • What makes this important?
Follow-up	• Is there anything one should avoid communicating?

Participant's own work on security requirements One of the main research questions of this thesis is to understand the current state of secu-

Table 4.6: Question 6: The communication of security requirements (Suppliers)

Question S	**What do you think is most important for you as a supplier for security requirements to communicate?**
Clarification	• Is it concrete functions, or e.g. security goals? • Why? • What makes this important?
Follow-up	• Is there anything one should avoid communicating?

rity requirements in public procurements. This section of the survey asked participants about their own work with security requirements, with the goal of understanding how security requirements are designed, interpreted and implemented.

In question 7, given in Table 4.7, the specific procedures used to write security requirements is the focus. The objective was to get the participants to talk about their work on security requirements, and through this gain an understanding of any methods and procedures used. As the prospect of reusable requirements was of interest, there were several clarification questions regarding this topic.

Table 4.7: Question 7: Procedures for writing security requirements

Question P	**How do you proceed to write security requirements?**
Clarification	• Can you describe the process in more detail? • What do you use as a basis when you write security requirements? • Do you reuse security requirements from earlier projects?
Follow-up	• What is the reason for using this process?

As security is only part of the bigger picture in a software development project, it was interesting to get the participants' opinions on the overall importance of the security requirements. Question 8 (Table 4.8) looks into how central security requirements really are in the process of writing the requirement specification. It would not be surprising if the participants of this study - security operatives - were of the opinion that security requirements are important for IT-systems. Therefore, it was valuable to ask about the state of practice, and understand where on the list of priorities security requirements usually end up.

Table 4.8: Question 8: The importance of security requirements in the requirement specification

Question P	**How central are security requirements when the requirement specification is written?**
Clarification	• When in the process are security requirements developed?
Follow-up	• *Relate to the answer given by the participant on question 2.*

In the prestudy, several systems were found to have few or no security requirements. This motivated question 9, asking whether the security requirements set in the tender documents represent the actual security delivered in the final systems. As seen in Table 4.9, the question was formulated a bit sharply using the word *only*. The goal was to make the participants think about their stand on this issue and then being able to ask for the reasoning behind. Should the question not be understood, the clarification question was more blunt, asking whether there were incidents where more security than asked for had been delivered.

Table 4.9: Question 9: Limitations put on security by the requirements

Question P	**Is it your experience that you only get the security you ask for?**
Clarification	• Are there times when you are delivered more security than you asked for in the tender?
Follow-up	*No follow-up questions*

With the same motivation as for question 9, question 10 (Table 4.10) relates to feedback from suppliers on security requirements. When few security requirements are given, or the requirements are of low quality, it was interesting whether the procurers got feedback from the suppliers. Should that be the case, it might help mitigate some of the negative effects of poor security requirements. As communication is well regulated in the procurement process, the clarification question inquired about the possibility to give feedback when the supplier had been chosen, and had started their work.

Table 4.10: Question 10: Feedback from suppliers

Question P	**Do you have any examples of feedback from suppliers on the security requirements you have made?**
Clarification	• Either in conjunction with the procurement process, or during implementation?
Follow-up	Is it usual/possible to receive feedback from suppliers on requirements that are set?

Questions 11, 12 and 14 are very similar to questions 7, 9 and 10, but were modified to be asked to suppliers instead of procurers. Instead of asking the suppliers of the importance of security requirements when the requirement specification is written, as done in question 8 (Table 4.8), the suppliers were asked about their general opinion on the quality of security requirements in question 13 (Table 4.13).

Table 4.11 presents question 11, which was aimed at understanding the process of security requirement fulfilment. Together with question 7, this question aimed to understand how security was ensured, from requirements to the actual implementation. When the process that creates security features is charted, it will be possible to understand how improvements to the work on security can be done.

Table 4.11: Question 11: Procedures for fulfilling security requirements

Question S	**How do you proceed to answer/fulfil security requirements?**
Clarification	• Can you describe the process in more detail?
Follow-up	• *No follow-up questions*

Question 12, given in Table 4.12, is similar to question 9 (Table 4.9) asked to the procurers. The theme is whether security is limited by the requirements set in the requirement specification, or if it is usual (or even possible) for suppliers to deliver more security. Should there be discrepancies between the procurers and suppliers on these questions, there could be a risk that the security of publicly procured IT-systems is not as good as procurers expect.

Table 4.12: Question 12: Level of security provided by suppliers

Question S	**Do you only implement the security the customer asks for?**
Clarification	• Do you sometimes evaluate the security requirements as bad, and implement more than is asked for?
Follow-up	• How does broad/vague security requirements affect the security that is delivered?

The prestudy revealed large differences in quality between security requirements. With question 13 (Table 4.13) the goal was to get the suppliers' view on the security requirements they see in their work with tenders. It was possible that they support the conclusions of the prestudy, but it could also be the case that they felt that the current state of requirements was sufficient.

Table 4.13: Question 13: The quality of security requirements answered by suppliers

Question S	**How do you view the security requirements you partake in answering?**
Clarification	• Can you say anything in general about the quality? • How easy are the requirements to understand?
Follow-up	*No follow-up questions*

Question 14, given in Table 4.14, is identical to question 10 (Table 4.10), with the only change being that it was adapted to suppliers. It was interesting if the suppliers felt that they provide feedback to the procurers, while the procurers don't share this view.

Finishing up the section on experiences with security requirements, question 15 (Table 4.15) pertained to the possibility for feedback on security requirements. As such, it was related to question 10 and 14, but rather than asking about examples, the question focused on the opportunities for communication inherent in the process of procurement. Participants might have already answered this through the previous questions, but it was important to ensure that this theme was covered before the interview moved on. A clear possibility to communicate and clear up misunderstandings could go a long way in mitigating some of the issues identified in the prestudy.

Table 4.14: Question 14: Feedback to procurers

Question S	**Do you have any examples of feedback you have given procurers on security requirements?**
Clarification	• Either in conjunction with the procurement process, or during implementation?
Follow-up	• Is it usual/possible to give feedback to procurers on requirements that are set?

Table 4.15: Question 15: Communication between procurers and suppliers

Question	**What opportunities are there for communication and feedback on security requirements between procurer and supplier?**
Clarification	*No clarification questions*
Follow-up	• Is this opportunity used? • Would you want more communication between procurer and supplier?

Evaluation of security requirements As described in questions 11 to 15 of the questionnaire (Figures 4.12 through 4.16), the participants were asked to rate four individual security requirements, and a group of requirements. In this part of the interview, the participants' answers to these questions in the survey were followed up. As the choice of which requirements to talk about would be done on an individual basis, the only question in this section, question 16, was very open. The main goal of this section was to get input on the attributes of the security requirements, as they were constructed based on the conclusions of the prestudy. Consequently, the feedback on the requirements would be relevant as feedback on the general principles the requirements represented.

Table 4.16 shows the open ended question asked in this section. Other than the formulations written down, this part of the interview had to be adapted to each participant, rendering any work on more general statements of little value. The clarification questions had to be adapted with information from the questionnaire, using both the participant's own answers, but also the aggregated results from all participants.

Table 4.16: Question 16: Open questions on security requirements from the questionnaire

Question	**What are your thoughts on this security requirement?**
Clarification	• You have answered ... Can you clarify why you think this is the case? • Compared to others ... What are your thoughts on this difference?
Follow-up	• How would you formulate a similar requirement?

Closing general questions Approaching the end of the interview there were four questions that were more open to interpretation for the participants. Having more open questions at the end allows the participants to focus on areas they find interesting and important, making them comfortable and keeping their interest. It was also possible that the participants would have been triggered to think about different security related topics during the interview, and this gave room for these thoughts to surface.

Question 17 (Table 4.17) relates to the development in the state of security requirements over time. Should the study find that security requirements in general are in a bad state, reports of a positive development will be encouraging. As the prestudy showed, there are many categories of security requirements, and it was interesting to find out if they had all become more important, or if there were differences between the different types of requirements.

Table 4.17: Question 17: The development of security requirements over time

Question	**Do you think security requirements have become more important the last years?**
Clarification	• Why? • Are there any specific areas that have become more important?
Follow-up	*No follow-up questions*

Having talked to the participants for some time, it was interesting to have them describe their thoughts on high-quality security requirements. Question 18 is quite blunt but open in asking this, as seen in Table 4.18. Here, the participants were given room to move the discussion in a direction they felt was important or not yet covered. Some participants might have felt that the topic was already covered, and the clarification questions were meant to make the participants reflect on attributes that should or should not be included in a good security requirement.

Table 4.18: Question 18: Good security requirements

Question	**What do you think is a good security requirement?**
Clarification	• What are the attributes of a good security requirement? • What should be avoided in a good security requirement?
Follow-up	*No follow-up questions*

With the large differences in quality of security requirements found in the prestudy, a question that had manifested itself was whether the security requirements are defining for the security of a system. Is good security just expected by the procurers, and delivered without question by the suppliers, or is the specification of such requirements paramount to the final security of the system? Question 19, as seen in Table 4.19, put this forth as a straight yes/no question. Doing so was not in line with the theory, as it might make the participants answer only yes or no. As this was well into the interview, the participants were hoped to have open up enough to themselves elaborate on the subject. If not, there were several clarification questions on hand to move the conversation along. The goal of a yes/no question at this point was to get clear opinions from the participants, while they could still follow up with explanations. The theme of the question is important, and clear answers were therefore preferred.

Ending the prepared questions, the opinions of the participants on the overall theme of security work within the limitations of the public procurement framework was interesting. Table 4.20 shows the final question of this section, asking the participants what they felt could be done about the public procurement process. The clarification question asks whether checklists and recommendations can help procurers and suppliers to create and fulfil security requirements in a better way. Getting the participants' input on this was vital, as they are the ones who know if such tools will be of any help.

Closing questions In finishing up the interview, two open questions were asked to the participants. The first, shown in Table 4.21, gave the partic-

Table 4.19: Question 19: Importance of security requirements

Question	**Is it the security requirements that decide if we get good security in our solutions, or are there other factors?**
Clarification	• (If no:) Should we then be focusing so much on security requirements? • What should we be focusing on instead? • (If yes:) Do we then have enough focus on security requirements? • How can we ensure that security requirements are central in the procurement process?
Follow-up	*No follow-up questions*

Table 4.20: Question 20: Simplification of security requirements work

Question	**What can be done to simplify the work with security requirements in public procurements?**
Clarification	• Can the development of good guides, simple recommendations or sample requirements help?
Follow-up	*No follow-up questions*

ipants the opportunity to talk about anything related to the overall theme of the study that had not been covered yet. The participants in the study are experienced and knowledgeable on the subjects of information security and public procurements. Providing them with the opportunity to freely talk about the themes they find important was seen as valuable. It also made the interview end with a question where the participants were in control, which would hopefully leave the participants with a good feeling.

Table 4.21: Question 21: Open question on the themes of the study

Question	**Do you have anything else you would like to talk about, that you don't feel you have had the opportunity to talk about so far?**
Clarification	*No clarification questions*
Follow-up	*No follow-up questions*

The final question was related to the privacy and data collection done in the study, and is shown in Table 4.22. It was important to give room for any concerns the participants might have about these subjects.

Table 4.22: Question 22: Open question on the privacy and data collection of the study

Question	**Do you have any questions, either about the study, data processing, or something else?**
Clarification	*No clarification questions*
Follow-up	*No follow-up questions*

4.3.3 Conducting the interviews

When carrying out interviews, there are several factors that must be taken into account to ensure that the participants are comfortable and willing to share information. The main factors considered in this study is presented in this section.

Interviewer skills While it is not feasible to expect to be able to gain many new skills in the short time given for a master's thesis, it is interesting and important to be aware of skills that are considered to be of value to an interviewer.

Being a good listener who is able to use the information given to move the interview forward, having a good memory to tie together strings from different parts of the interview and other interviews, as well as having a clear mind capable of simultaneously conducting the interview, writing notes and formulating the next question, are viewed as central skills for an interviewer. Having a curious mind and a strong interest in the field in question are seen as qualities that will help the interviewer gain these skills. [31]

High-status interviewees [39] describes a situation where the person being interviewed has a high status, and how this can be a difficult situation for the interviewer. As most of the people that were recruited to this survey are expected to hold quite high positions in the firms and organisations they work for, this became relevant. The two possible pitfalls described are for the interviewer to attempt to show off their knowledge in the subject matter, and through this offend the participant, or to be too nervous or unknowledgeable, and as such be patronised by the participant [39]. Succeeding in this balancing act was important, as it is key to establish a good rapport with the participants, and thus getting relevant and truthful answers.

Difficult interviewees There are mainly two types of interviewees that are described in the literature as problematic, the quiet or uncommunicative participant, and the dominant or over-communicative participant. Handling the quiet participants is usually done by building a good rapport, using a lot of prompts, and rephrasing questions to make them difficult to answer in just a few words. The dominant participants can be more difficult. In the semi-structured interview, there should be room for digressions as this can be the basis for discovering new and interesting subjects and themes. If there is a need to guide the participant back on track, this must be done carefully, making sure it is not viewed as disinterest. One strategy is referring back to something interesting the participant has talked about earlier in a natural pause. [31, 39]

Participants putting on a front In a couple of the interviews, there were tendencies that the participants were putting on a front, as described in [34]. The participants took on a role where they were telling a story of how good their system was, when the actual question was about the general state of the business, or otherwise not related to the specific systems of the organisation.

The recommendation for these kinds of situations is to stop doing follow-up questions, as there is a low likelihood that the participant will actually provide relevant answers. Instead, the topic should be abandoned, and if possible visited later. [34]

In the instances where this happened, the interview was moved on after trying to rephrase the question, as to make sure that the case was not that there was a misunderstanding on what the actual question was.

Recording Conducting semi-structured interviews without making recordings of the conversations is a nearly impossible challenge. The risk of losing vital information from the participants when making notes is imminent, and with the certainty that the participants would have significantly better domain knowledge than the author, the need for recordings was clear. Making recordings during interviews can be a challenge, as the participants might see this as threatening, be less willing to be honest in a fear that the recordings might leak, and in the worst case, it might cause participants to withdraw [32].

Ensuring that the material from the interviews would be recorded correctly was of utmost importance in the study. The main mitigating measure taken was the use of two different recorders. One recorder used a built-in microphone and chargeable battery, while the other had replaceable batteries and an external microphone. This ensured a backup in case one recording was lost, got corrupted, or one of the recorders did not record correctly. It did, however, introduce an extra potential stress element for the participants, as the presence of just one recorder can be off-putting enough. This was handled by telling the participants the exact reason for the dual recordings, and with the use of a bit of humour. No participants objected to the recordings, though some participants did volunteer more information when the recorders had been turned off and put away. Where relevant, this was noted in the written notes for the interview.

Note sheet Even though the interviews are recorded, notes should be taken during the interview. The notes are a backup in case the recordings are lost, or unusable, and the act of taking notes forces the interviewer to focus on what the participant is saying. With the interview guide as a starting point, each question was placed to the left of the page, and the space used for clarification and follow-up questions was freed to make room for notes. Making the note sheet in this way allowed the interviewer to see the questions while making notes, and as the note sheets were in the same format as the interview guide, keep track of how far the interview had progressed.

Scheduling and location As the participants interviewed are busy people, and under no obligation and with little incentive to participate in the study, it was important that the interviews were conducted on the participants' terms. For the participants' convenience, the interviews would take place at their place of work. This was also beneficial as there would be no need to get a dedicated office to conduct the interviews, and because the participants would be on familiar ground. Making the participants comfortable is important, and they are more likely to feel in control and relaxed in a known environment [33].

A possible problem with this is the proximity to the everyday environment of the participant, which might become a distracting factor, and there might be interruptions. There might also be a lot of environmental noise, making the recordings difficult to transcribe. [40]

Planning the interview schedule required a lot of back and forth communication with the participants. As discussed, the participants in the study are people with a tight schedule, and taking part in a study conducted by a student is of course not on the top of their list of priorities. In spite of this, only one interview had to be rescheduled after first being agreed upon. One of the interviews, where two people were supposed to participate, had one of the participants cancel, but the interview was still conducted with the remaining person.

As the interviews had to be conducted at the workplace of the participants, the scheduling process also had to take into account time for travel, and finding the way to each office. Consequently, no more than two interviews were set for each day, and a solid buffer was placed between the interviews. This was done not only to give peace of mind during the interviews, but also to take into account that the participants might be delayed for the interview, and thus having time to conduct the full interview nonetheless.

Time restraints Continuing the challenges from the previous section, it was expected that some participants would not have time to complete the entire interview. The participant might inform the interviewer of this ahead of time, or this might come up at the start of the interview. Due to this, the interviewer should have an idea of which questions are most important, and which can be skipped. This is also useful if the participant talks a lot, or some other theme is discovered during the interview, and there is little time left for the planned questions. [34] argues that it is not a big problem if one participant does not answer all the questions, as there are many others who can provide insight into the themes foregone.

One of the interviews were shortened by 15 minutes at the participant's request. The request was given ahead of time, and as such the interview guide was updated, marking the most important questions. As the interview in question was around the middle of the study, some questions had been answered by many participants, while others had few or contradictory answers. Questions lacking information, or with no clear consensus were prioritised.

4.3.4 Post interview work

When the interviews are finished, the work of identifying the relevant information in the collected data begins. The main activities in this work, transcription and coding, are presented in this section.

Transcription Extracting the data in the audio recordings was done through the process of transcription, writing down word for word the audio recording of the interview. This is a time-consuming process, requiring high levels of concentration for extended periods of time.

One common pitfall in transcription is the misinterpretation of the audio recording, or the mistyping of the participants' statements, which can cause the meaning to change. This is potentially very damaging to the end result, as the data of the study is distorted. The main tactic recommended to avoid this is for the researcher to personally transcribe the interviews.[40]

Before starting the interview process, Daniela S. Cruzes, a research scientist at SINTEF in Trondheim was contacted to discuss the process of interviewing and transcribing. She recommended estimating about 5-8 hours of work to transcribe and code 1 hour of recording. This limited the number of participants that could take part in the survey. With 45 minute interviews, 20 interviews could give a total of 120 hours of post interview work just to extract the data. [40] also strongly recommends the use of specialist transcription equipment such as a foot pedal which controls playback of the recording.

After conducting the interviews, transcriptions were conducted as quickly as possible, to ensure that the interviews were fresh in memory. On average, the transcriptions were completed at a ratio of 1:3, that is one hour of recording took 3 hours to transcribe. This was a promising development, as it is far faster than was estimated at the beginning of the project, as well as being below the estimates of Daniela Cruzes. The use of a pedal to control playback was not possible, as NTNU did not have such equipment on loan to students at the author's institute. Instead, a transcription software which supported global hotkeys was used, enabling the transcription to take place in a suitable writing program, while both playback speed, reverse and fast forward could be controlled using the keyboard. This greatly increased the transcription speed.

The audio quality of the recordings was problematic for several of the interviews. As some interviews had to be done in more public spaces with a lot of background noise, this was to be expected, but there were also great differences in the quality of the two different recorders. Luckily, the recorders had different strengths, making it possible to find the best recording to listen to for each interview.

At some points, it was problematic to understand the participants while listening to the recording. Using the notes taken during the interview, changing the recording that was listened to, and listening repeatedly at different speeds, most of these instances were resolved. Where this was not possible, the transcript was marked to indicate that the audio was inaudible.

Coding Coding is the process of going from the raw text of the transcripts to finding topics and concepts in the interviews. This is done by marking the transcripts of the interviews with all occurrences of the topics, usually with a code (thus the term). The text from the interviews are processed, and anything related to a specific topic or subject is marked with the same code. This can now be extracted across all the interviews, and processed separately. Doing the coding correctly is important, as it shapes the data that can be retrieved from the information at hand. If a concept is not identified at the time of coding, it will not be possible to investigate this further, causing the conclusions to be affected. [34]

The coding process starts by reading through the interviews, taking notes of commonly occurring or interesting topics and quotes. Using this, as well as suggestions from the literature, the questions from the interview guide and common sense, topics are identified. In addition, it is recommended to use the list of topics to attempt to find new topics, e.g connections between the existing topics, or opposites. [34]

When a set of topics have been defined, it is important to make a clear and consistent definition of these, and the codes that will be used to mark up the text. One recommendation in [34] is to write down the definition of each code as such:

- What is it called?
- How is it defined?
- How will it be recognised?
- What will be excluded?
- What is a good example?

The definitions must then be used throughout the coding process, and should not be changed. Therefore, it is recommended that the definitions are tested on a sample of the text to check if the definitions hold up. When the definitions are finished, the interview text should be physically marked up, either in-line in the text, in the margin or using special software. [34]

Having coded all the interviews, the material must be analysed in order to extract the results from the interviews. This is done by looking the data identified for each code, and writing a summary of the results. Here, nothing should be left out, or viewed as more or less important, it is simply a summary of what has been said. With the summaries as a basis, it is possible to extract the most important topics. The topics that have been mentioned by the most people are expected to be both most interesting, and most likely to contain relevant results. In addition, there will be relations between topics that must be identified, such as opposites, and causes and effects. This must usually be identified based on the researcher's feel for the data, and as such, conclusions should be drawn with great care. [34]

Initially, after reading through the material several times, and looking at the research questions and the interview guide, 9 topics were identified for coding. However, after using these codes on a sample set of two interviews, one with a procurer and one with a supplier, the topic of *communication* had to be added, as it was not previously covered. The topic of the procurement process was originally only related to the *challenges* of public procurements, but in the sample set, there were both neutral and positive statements about the procurement process, causing it to be reworded.

Table 4.23 shows the final 10 topics that were identified and used for coding. In addition, everything related to the five example requirements described in Figures 4.12 through 4.16 was coded as their own topics.

The coding was conducted by marking up the interview transcriptions in a specialised program capable of extracting all text marked with the same code.

Table 4.23: Topics identified for coding

#1 The procurement process

Definition: A limitation or advantage to the process of acquiring the specified system due to the rules and regulations set for procurements. Everything directly related to the rules and regulations of procurements.

Recognition: Talks explicitly about the laws and regulations or challenges that are objectively caused by the procurement process. Includes activities dictated by the procurement process, such as competition types.

Exclusions: Does not include challenges that are present in projects that do not follow the public procurement rules. Does not include the attributes of specific requirements, this is part of #5

Example: Supplier describes how the process of asking questions regarding the contents of a tender reveals business internal information, as the questions and answers are disclosed to all participants.

#2 Reusable requirements

Definition: A requirement or set of requirements that are meant for use in more than one system, or that are identified as useable in new systems.

Recognition: Talks explicitly about requirements that can be used again, or talks about checklists, requirement databases or other tools for reuse of requirements.

Exclusions: Requirements that are required by law or regulations.

Example: Procurer describes how requirements for backup and logging are standard for all systems, and can therefore be added to any requirement specification.

#3 Use of standards

Definition: The use of a well defined standard for security requirements or practices.

Recognition: Talks about standards, or refers to requirements that are part of well defined standards.

Exclusions: Excludes internal guidelines and internal standards, these are part of #4.

Example: Talks about how the organisation implements ISO27000-family.

Table 4.23 – continued from previous page

#4 Methods and frameworks for security

Definition: Internal or external methods and framworks employed to formalise the creation and fulfilment of security requirements.

Recognition: Talks explicitly about framworks or methods used to write and fulfil security requirements. Describes formalised methods or written down procedures for eliciting or fulfilling security requirements.

Exclusions: Excludes any well known standards, these are part of #3.

Example: Describes an internal process that requires elicitation of requirements from all stakeholders before security requirements are written.

#5 Requirement attributes and literature recommendations

Definition: Attributes of security requirements, either specific or in general terms, as well as anything relating to the recommendations given for security requirements identified in the literature.

Recognition: Talks about the attributes a security requirement should or should not have. Describes or talks about the recommendations found in the literature, either explicitly or implicit.

Exclusions: None identified.

Example: Participant describes the problems of requirements that are too broad, and thus are difficult to evaluate.

#6 Competence and resources

Definition: Competence in the field of information security, available resources both in terms of time and money, and knowledge in the business as a whole.

Recognition: Talks about resource scarcity or cost of requirements or competence. Includes education of the rest of the organisation on matters of security and evaluation and follow-up of tenders.

Exclusions:None identified.

Example: The procurer describes lack of resources to be sufficiently able to evaluate the security of the end product.

Table 4.23 – continued from previous page

#7 Security work
Definition: The security related work in the organisation, its development and importance. *Recognition:* Talks about how the organisation works with security and the importance of security. *Exclusions:* Excludes anything that can be placed in other categories. Statements about the work to create an internal checklist for security should e.g. be categorised as #4. *Example:* Procurer describing how the organisation has grown to see security as much more important in the last years.
#8 Certifications
Definition: Certifications in international standards, or other external certification programs. *Recognition:* Talks about the certifications of the organisation, the merits of certifications, or the content of certifications. *Exclusions:* Does not include requirements for certification, these should be categorised as #5. *Example:* Supplier explains why being certified not necessarily makes them more attractive as a supplier.
#9 Experiences
Definition: Actual experiences and stories about security requirements. Empirical events. *Recognition:* Is not an opinion, but rather an actual event or experience the participant has been part of or heard of. *Exclusions:None identified.* *Example:* Procurer has experienced that using a small supplier is worse for security than using a large.

Table 4.23 – continued from previous page

#10 Communication
Definition: Communications between suppliers and procurers relating to security requirements, the procurement process or the system in question.
Recognition: Participant explains how communication is done, and what is communicated. Includes both oral and written communication.
Exclusions: The publishing of the tender document is not seen as communication.
Example: A supplier describes how questions are asked after the tender is published.

After coding the material into the aforementioned topics, a summary for each topic was written. This made it possible to gather all information provided by the participants on each topic. In addition, it facilitated the understanding of what claims were supported by several participants, and where there were opposing views. While the coding process should have coded all statements correctly, it turned out that some of the statements overlapped several topics. This made it necessary to write some of the summaries simultaneously, switching between them as information that was relevant to another topic was found.

In addition to the topics that were identified for coding, a summary was written for the topics of *small and large suppliers*, *the governmental standard contracts (SSA)* as well as one for memorable quotes.

4.4 Alternative methods

In the study conducted, the chosen research methods were an online questionnaire and individual semi-structured interviews. There were several alternative research methods that could have been used, and the reasoning for not doing so is given here in brief.

4.4.1 Group interviews

One very similar research method to the individual interviews conducted is group interviews. Here, a number of people are gathered and interviewed together, allowing them to discuss in the group. As the people recruited for this study have been very enthusiastic about their field of work, this could have led to some very interesting discussions.

The concern for the participants' anonymity, and the sensitivity of the topic at hand did however not favour this method. It was feared that recruitment would be more difficult, and that participants would not volunteer as much information if it had to be shared with other people than the interviewer. In addition, the scheduling would have been even more complicated, and would have required some of the participants to travel in order to take part in the interview.

As two of the interviews ended up being double interviews, the effect of this was observed during the interviews. The participants who were joined by a colleague were clearly engaging in discussions among themselves, providing interesting input that would probably not have come up had they been interviewed alone. These people were, however, co-workers, providing a different dynamic than discussing the theme with possibly unknown people from other companies.

4.4.2 Case studies

Another interesting research method considered was a case study of a couple of procurement processes. This would have required being present at the different parts of the process, with both procurers and suppliers, ideally in the same tenders. Doing so would have provided interesting insight into, and an outsider's perspective onto, the parts of the process rarely seen by the public.

There were however many challenges when considering this method. The biggest obstacle was time, as being part of the entire process from identification of need, to delivery and evaluation of product would not have been possible within the time allotted for a master's thesis. Being situated in Trondheim, with most governmental organisations and suppliers in Oslo would also reduce the number of possible projects. Performing this kind of field research would also run the risk of changing the behaviour of the participants, as they would know that the security requirements of the project were under particular scrutiny. Consequently, the results could have been rendered very weak.

4.4.3 Delphi method

A perhaps less used method is the Delphi research method, which gathers experts into panels, and sends them questionnaires in several rounds. Between the rounds, the questionnaires are revised based on the response from the previous round. Some of the main benefits of the method are that it allows participants insights into the feedback from other participants, and the opinions of the experts partaking can change and be further investigated during several iterations. [41]

While [41] argues that the method is well suited for graduate work, performing such a study in the time given for this thesis was deemed impractical. There was also a concern about how easy it would be to recruit participants to take part in such a study, as it requires commitment over time. [6] used the Delphi method when investigating procurement of IT-systems, and reported that the study had to be stopped after two iterations because several participants indicated that they would not take part in further rounds.

Chapter 5

Results and recommendations

This chapter will present the results of the study, as well as the recommendations given to improve the work on security requirements in Norwegian public procurements. The chapter starts with a presentation of the participant demographics in Section 5.1. Afterwards, the results are presented by topic in Sections 5.2 through 5.5. For each topic, the contributions of the participants are presented, followed by a recommendation for improvement. Section 5.6 presents other interesting findings done in the course of this study. These findings are reported and discussed, but no recommendations are given. The chapter is concluded with a description of the limitations of the study in Section 5.7.

5.1 Participant demographics

To be able to interpret the results, it is important to get an understanding of the participants in the study. The first part of the questionnaire, as described in Section 4.2.2, asked the participants about their experience with security requirements, as well as certifications and education.

The participants were divided between having experience with writing tenders and answering tenders as shown in Figure 5.1[1]. In total, 12 interviews were conducted, and counting the two double interviews 14 people participated in the study.

The people participating in the study represents supplier and procurer organisations as seen in Figure 5.2. While the distribution of organisations is interesting, it is important to note that it is the personal experience of the

[1] The experience shown is based on the answers from the interviews. The placement of a participant into a category has been done on the basis of the experience the participant contributed with, not which fields they have been involved with in the course of their career.

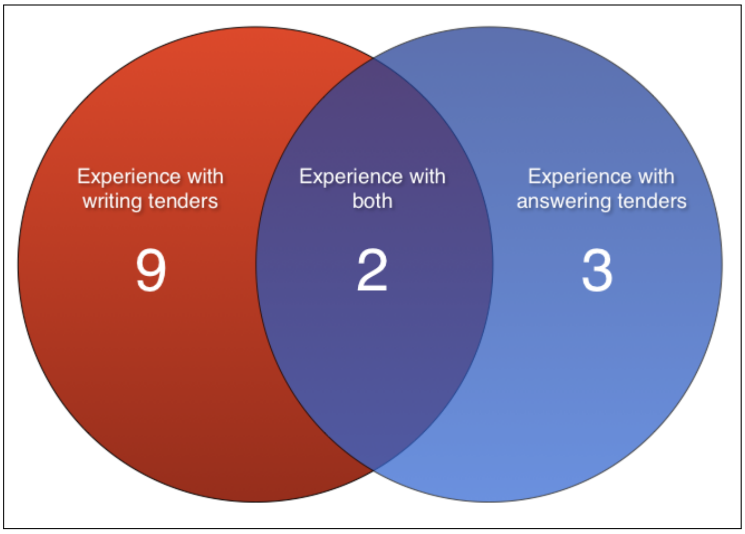

Experience with writing tenders
9
Experience with both
2
Experience with answering tenders
3

Figure 5.1: Participant experience based on actual contributions, shown as a venn diagram

participants that adds value to this study. As such, a participant's place of work is not material to the contributions made. There is however expected to be a skew in focus towards the type of organisation the participant is currently employed in, especially as they are interviewed at their place of work. Additionally, it would not be unreasonable for participants to feel that they were interviewed in the capacity of their current position.

When asked to estimate the number of tenders they had participated in either writing or fulfilling, the average for the procurers was 24, and the average for the suppliers was 22.

Seven of the participants reported that they had no certifications in IT-security. For the six participants reporting certifications, ISO 27000 family certifications were most common. In total ten different certifications were reported.

Only four participants reported no form of education or courses in security. Of those reporting such activities, external courses were the most common form of education on security, followed by internal courses and security courses during formal education. The number of participants that reported the different forms of education are shown in Figure 5.3.

Because of the way the participants were recruited, it comes as no surprise that most of them have extensive experience with security work and tenders. Participating in a study about security requirements is probably not of interest to people who are aware of large flaws in their organisation's security

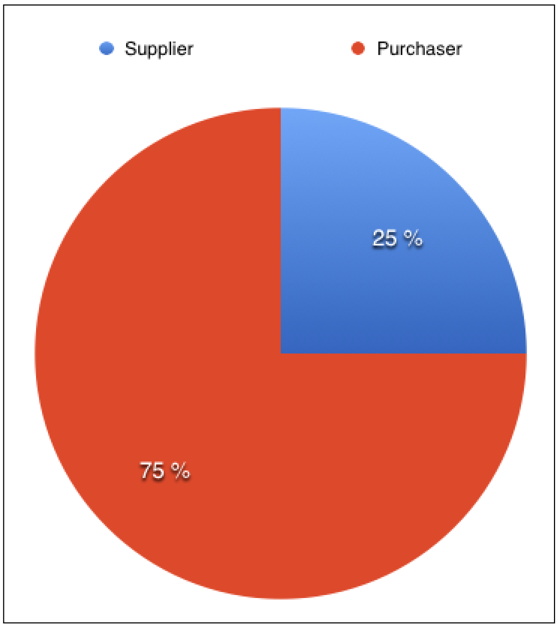


Figure 5.2: The distribution of participant organisations between suppliers and procurers

practices. Altogether, the participants should not be seen as a representative selection of the security operatives in Norway, but are rather expected to be in the high end of competence and security focus. This impacts the results in two main ways: (i) The reported attitudes on properties of security requirements and how security work should be done, will most likely be of high quality, and (ii) The reported level of competence and security focus will probably be higher than can be expected if a random sample of security operatives were surveyed.

The makeup of the participants should be taken into account when using the results of the study.

5.2 The procurement process

The central goal of this study has been to find out whether the procurement process itself causes any challenges for security requirements in publicly procured IT-systems. This has also been one of the primary areas of the interview guide, and it is therefore no surprise that this is one of the themes the participants had most to say about. Specifically, five areas will be discussed in detail: the attributes of security requirements, how security

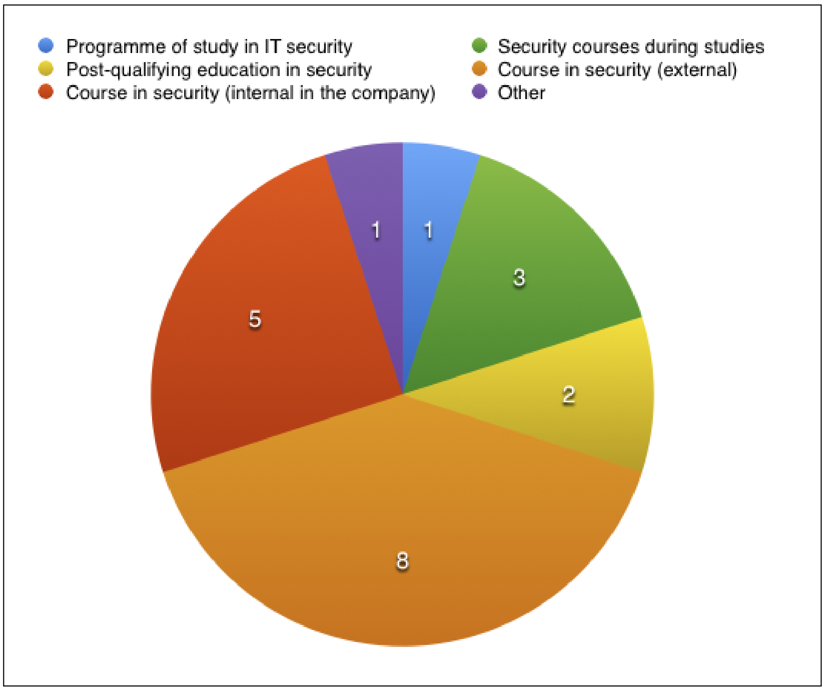


Figure 5.3: The education reported by the participants

requirements must be adapted, the required transparency of the procurement process, limiting factors in the amount of security requirements that can be set, and the type of competition used in the procurement process. Finally, a recommendation for the use of negotiated processes is given.

5.2.1 Requirement attributes

A central theme to all the interviews has been how security requirements should be phrased to ensure that they contribute to better security. It is clear that the balance between too vague and too strict requirements is seen as difficult. If requirements are too specific, one faces the risk of excluding suppliers that have solutions which are fitting for the organisation, but solve the challenges in different ways than the procurer imagined. Several participants pointed out that the procurement process is in place not only to ensure fair treatment of all suppliers, but also to allow the suppliers to show the procurers what is possible.

> ”We must entrust the marked to actually provide us with the knowledge of what is a good solution or a good service.”
> - Procurer

Given too specific requirements would result in many suppliers dropping out, causing the procurer to be forced to choose between the remaining few, or only remaining, supplier. This leads to little choice in technology, as well as allowing the suppliers to dictate the price.

One of the suppliers also said that very specific requirements would usually provide opportunities for additional sales, as the customer would understand that they have other needs later in the process, thereby causing change orders to be issued.

> "As a supplier you would say that this is good stuff, as there is absolutely possibilities for additional sales." - Supplier

Due to this, tenders with very strict requirements could be seen as preferable to the suppliers, as there is a huge potential for further orders, and therefore a financial upside.

Should no providers be able to fulfil the strict requirements set, the competition must be cancelled and a new competition announced, an expensive and time-consuming process.

Question 12 of the survey, given in Figure 4.13, asked the participants to rate a security requirement constructed to be very specific. The requirement was rated by most participants to be neither good nor bad. When asking some of the participants about the requirement, they seemed to find it too specific, while at the same time being positive to a requirement on transport security.

On the flip side are requirements that become too broad, and allows room for interpretation exceeding the procurer's intentions. The prestudy found several instances of very broad requirements regarding best practice and compliance with laws and regulations, exemplified in question 13 and 14 of the questionnaire as seen in Figures 4.14 and 4.15. One of the questions posed to several of the participants during the interviews was whether this could act as a legal shield for the procurer, shifting any blame for unwanted incidents to the supplier. Both procurers and suppliers were in agreement that this hurts the procurer the most. The suppliers' perspective was that this is something suppliers would protect themselves from during contract negotiations, thus nullifying any intended legal shield. From the procurer side, these kinds of broad requirements are seen as bad because it can be just as easy for the supplier to claim that their system fulfils an interpretation of the requirement, thus winning a lawsuit.

One way to help balance requirements that was presented by participants is to give the goal of the security in the tender documents. Providing suppliers with an understanding of each requirement, and how it helps security might make the requirements easier to understand.

The concern voiced by the participants on the balancing of security requirements between too broad and too specific, fits well with the findings of the prestudy [1]. [42] discusses how too specific requirements will impose restrictions on the development team, preventing them from using the best security techniques, while [5] makes the point that there is a real risk that no suppliers will be able to answer a tender with too vague requirements. None of the participants seemed to have a definitive answer on how to best handle this, other than being thorough in the requirement elicitation phase, presenting security goals, and having a constructive dialogue with suppliers.

The topic was nicely summarised by one of the participants:

> ”Too general requirements gives room for interpretations, we don’t want that, too specific requirements tie you down, that is not good either.” - Procurer

5.2.2 Requirement adaptations

In a related theme to the one above, there were several participants who reported that security requirements had to be adapted when a system was to be acquired through public procurement. The requirements must be altered to allow for true competition, making rigid requirements where the supplier must answer purely yes or no unsuited.

In addition, there were several procurers who reported that requirements might have to be withheld from the tender documents and added later, either in negotiations or in change orders, to ensure that suppliers are not discouraged from answering the tender. When asked if this was the case, one of the procurers answered:

> ”Yes, absolutely. And the same is actually the case for pure functionality. (...) to be able to reach the goal (...) you reduce on security requirements, you reduce on functional requirements (...).” - Procurer

The result, according to the same person, is that you are stuck with *”A bad product where you are at the supplier’s mercy when it comes to the price of change orders.”*.

It is clear that the procurement process can impede the procurers’ ability to set high-quality security requirements, as these requirements can end up being dropped to ensure competition for the tender.

5.2.3 Transparency

The public procurement process is built on transparency and equality, and requires the procurers to be open about the process. More specifically, any question that is sent in by a supplier must be published along with its answer, for all suppliers to read. Furthermore, when using a competition type involving dialogue the procurer must ensure that no supplier has received any advantage or disadvantage, and this must be documented through minutes from meetings.

The suppliers reported that asking questions in the time before the deadline to submit the bid is challenging. Doing so might reveal details about the bid to the competition, or make it possible for the competitors to gain an understanding of their level of knowledge on the subject. The result is that some questions are not asked, or the supplier might use other methods to get answers:

> "Since these are large governmental customers, we will always have one consultant that has worked with the customer before, and knows their architecture, and then we can, instead of asking questions, we can actually get that information." - Supplier

There are also transparency issues for the procurers. As the tender documents are usually public, the information contained in them becomes public knowledge. This is not always desired, especially with regards to security requirements, which may communicate too much about the internal security of existing systems. One of the procurers interviewed was very clear on the fact that the security requirements should not reveal anything about their systems:

> "That would have been a disaster. Then anyone could have joined the competition, become pre-qualified, and then get that information." - Procurer

It also seemed normal for tender documents, also those that are only issued to pre-qualified suppliers, to be spread to other customers as examples of how to write requirements. Including the fact that most tender documents would be handed out as the result of a freedom of information request, the information in these documents can not communicate anything security-critical.

The transparency issues that have come to light in the study may pose a risk to the security work in IT-projects. Suppliers do not feel comfortable asking questions that could impact security, and the procurers are not comfortable sharing such information until very late in the procurement process.

The consequence of this might be that the security requirements are either misunderstood, given too low priority, or introduced at a too late stage in the development process.

5.2.4 Number of requirements

When deciding on the security requirements to be included in the requirement specification, there is a need to consider how many requirements can be included. Several participants explained that including too many security requirements makes each requirement insignificant, and thus easy to ignore by the suppliers.

A participant provided an example for the weighting during evaluation of bids, which is shown in Figure 5.4. 50% of the evaluation is placed on functionality, 30% the ability to complete the project and 20% price. The block of functionality is then broken down into 60% functional requirements, 20% architecture and 20% user friendliness, performance and security. In total, 3% of the evaluation is then placed on security. If security is then specified in 20 requirements, each requirement constitutes 1.5‰ of the total score, making it easy to ignore one or more of them, while still winning the bid, given that the security requirements are not mandatory.

This is especially a problem for security requirements as they are expensive to implement, making dropping a (non-mandatory) security requirement to be able to lower the price a good choice for the supplier. Solving this would require all security requirements to be set as mandatory, something that would probably cause further challenges, or weighting security requirements more heavily in the evaluation of tenders.

5.2.5 Competition type

One of the issues where there seems to be great agreement is the need for dialogue based procurement processes when acquiring IT-systems. While procurement with dialogue was reported as a resource intensive process to complete, it gives a greater amount of control to the procurer. Being able to discuss with the suppliers how their solutions work, and give feedback on any parts of the tender that have been misunderstood or are not sufficiently covered in the proposed solution, is seen as valuable.

The procurers reported that using a competition type with negotiations reduces the project risk, though not to the extent that the risk for a bad final product is reduced significantly. Even with dialogue and negotiations, the need for quick results, as well as financial motives, makes security a low priority in many projects.

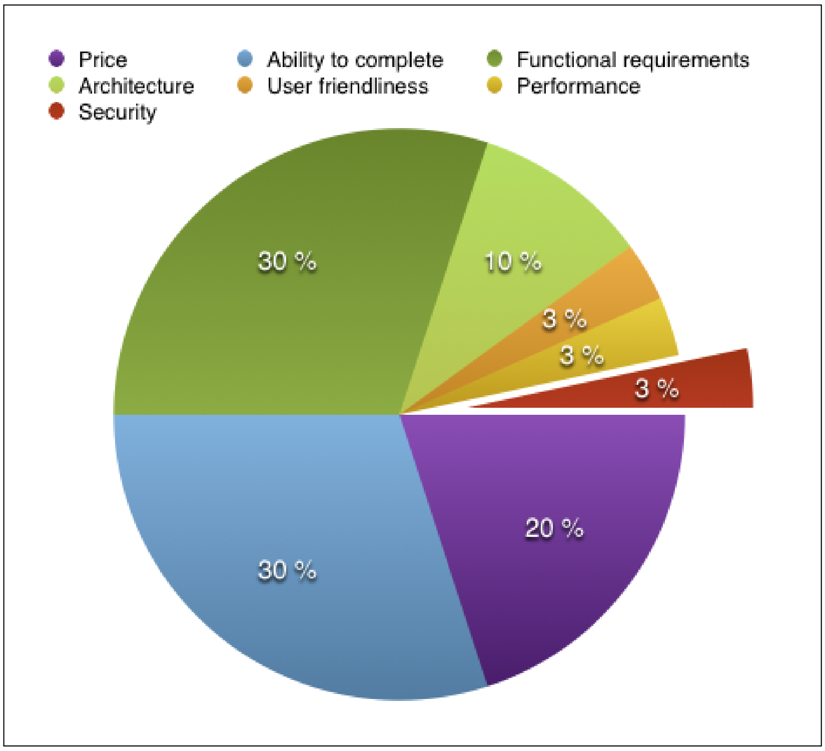


Figure 5.4: An example of the percentage weight for each category when evaluating a bid

The suppliers seem to agree with the notion that dialogue is important:

> "[in a previous job] security was very central to a delivery (...) and dialogue meetings were used. This was also crucial to the customer's success." - Supplier

Many of the obstacles caused by the procurement process are viewed as solvable, or at least easier to solve, given that a dialogue is allowed. When encountering a security requirement that is either difficult to understand, or seen as unnecessary, this can be addressed in a meeting with the procurer.

Reviewing the answers from the interviews, it is clear that one of the tools both procurers and suppliers would like to see used more often is competitions with dialogue. The alternative is for the supplier to either make guesses on the procurer's needs or to not answer the tender. Suppliers deciding not to provide a bid reduces the competition for the tender, possibly leading to higher prices and poorer solutions. While dialogue is not a *silver bullet* for handling security requirements in public procurements, it is clearly a tool that is used too infrequently.

5.2.6 Recommendation

It is highly recommended that procurers shift tenders for IT-systems to negotiated processes, especially for systems that are security-critical.

It has become clear through the interviews that both procurers and suppliers prefer competitions that include the option of negotiations. The main reason for this is providing the suppliers with an opportunity to ensure that the bid is in line with the customer's wishes, and for the procurers to clarify requirements. Negotiated processes are more demanding for the procurer, and have strict rules to ensure equal treatment of all participants. There are also larger costs associated with the bid for suppliers, who spend more time on the bid, thus losing more money if the bid for the tender is unsuccessful.

The advantages of negotiated competitions outweigh the downsides, as many of the challenges in procurement processes are easier to overcome in a negotiated competition. Importantly, the issue of balancing security requirements between being too broad and too detailed can be, at least partially, mitigated by better dialogue between the parties of the tender. Additionally, the transparency issues can be handled better with a negotiated process, and there should be less need to make adaptations of requirements for the sole purpose of attracting more suppliers. As this study has shown, the aforementioned challenges may impact the security of IT-systems purchased by the government, and making it easier to deal with these areas should improve IT-security.

5.3 Reusable requirements

Many of both the suppliers and procurers that were interviewed expressed the need for, and usefulness of, standardised security requirements or checklists. The use of such tools was reported to help compensate for the short time available to write the requirement specification, and in some cases for the lack of security knowledge in the organisation. Three main themes were of interest concerning this subject and are presented in the following sections: the development of standardised checklists, gaining a common vocabulary, and the current state of practice. Finally, a recommendation for the development of standardised checklists is given.

5.3.1 Standardised checklists

One of the solutions for the current state of security requirements brought up by several participants, was the creation of a standardised checklist to accompany the current governmental standard terms and conditions (SSA). Ideas for what such a checklist should contain varied. One participant wanted a checklist for different areas of information security, making the procurers aware of areas where security should be considered. Others wanted more specific lists of example requirements, or a minimum set of requirements that could become standard across governmental IT-procurements.

The participants viewed the checklist's main goal to be the establishment of a minimum level of security, and helping organisations without the necessary resources to reach such a level.

> ”(...) developing templates and checklists (...) makes the job easier for the organisations that don't have the competence or resources in this field, and we can at least get *some* security.”
>
> - Procurer

Reusable requirements present several challenges, including how detailed they should be, how standardised they can be, the necessary skills needed to use them and so forth. Regardless of the differences of opinion about the checklist's content, there was great agreement that any checklist or standardised requirements must be applied with care, and evaluated against each individual system. One supplier reported working on several tenders where the security requirements appeared to be a standard set that had been attached to the tenders without evaluation:

> ”A set of non-functional requirements that are stapled on at the back, and without any thought for what they mean, and they are not in accordance with the solution described (...).”
>
> - Supplier

One counter-argument brought up against the idea of a checklist of standardised requirements is the fact that the world of IT-security is extremely fast paced. The participant made the case that standards can create a false sense of security:

> ”I don't think there is a standard that can take care of all those things. In that case, I think that's a false security.”
>
> - Procurer

As security is a complex field, and must be adapted to each system, a truly standardised list will probably not be possible to make, nor wanted by the security community. The prestudy investigated three commonly used international security standards (Section 3.3.1.8), and identified 10 common areas of security requirements (Table 3.1). Using this as a starting point, a list of basic security requirements can be made, focusing on that which is most important to have in place with regards to security.

Another possible structure for this is a list of criteria for each area of security, with a recommendation that if a certain number of criteria are met, a security specialist is needed to evaluate the necessary security requirements. Such an approach would encourage custom security when needed, but not necessarily help organisations to improve security requirements on their own.

5.3.2 Common vocabulary

When discussing the theme of reusable requirements, a related theme surfaced: The need for a common vocabulary between procurers and suppliers.

> ”The main problem is the lack of harmonisation, there is no [universal language] the suppliers can relate to.” - Procurer

Many procurers have the same requirements but formulate them differently, forcing the suppliers to interpret whether or not the requirement at hand is substantially different from previously evaluated requirements. A harmonisation of requirements would remove this source of uncertainty, simplifying the process for the suppliers.

With more standardised requirements, suppliers would get accustomed to a baseline of security requirements, and their interpretation would be known. As a consequence time would be saved for the suppliers, and the procurers would get more reliable answers to the tenders, hopefully causing products to be delivered faster and cheaper. One of the suppliers supported this, while being reserved about the positive effects of the savings:

> ”If the public had standardised their requirements, it would have been easier for us, because when you have first provided an answer, you don’t have to spend time interpreting the security requirements in the next tender. But it’s not that big of a deal.”
> - Supplier

A common vocabulary would help suppliers and procurers better udnerstand each other, and might save both time and money. At the same time, this is not the central challenge in procuring secure IT-systems, but a part of the bigger picture.

5.3.3 Current state of practice

When conducting this study, several of the participants reported that their organisation was currently in the process of developing internal lists of reusable requirements, checklists or similar. Several others reported that their organisation already had this in place, and were actively using these in their projects.

How reusable requirements were implemented differed from organisation to organisation. Several procurers reported that they had a baseline for security, and a set of standard requirements to ensure that this was the case in all tenders. The reusable requirements that were reported seem to be a mix of requirements from standards the organisation use, baseline requirements for the organisation as a whole, as well as requirements that originate in experiences from previous systems. Some organisations had the application of these requirements as part of their information security management system, while others appeared to use more ad-hoc methods.

The participants seemed well aware of the fact that real security competence is needed to select the relevant requirements from the reusable ones. Understanding that reusable requirements does not replace local security knowledge was brought up several times in the interviews. The wrong selection of requirements can have a negative impact on the system, making local competence important.

It is clear that many public organisations today are developing reusable requirements to some extent. The main challenge seems to be that this is done in isolation, or with only minor input and sharing with other public organisations. Therefore, the wheel is reinvented regularly, and the collective security competence in the public sector is not utilised. A central set of reusable requirements could be developed by the top security operatives, and as such be much easier kept up to date and respond to new threats. It appears that the current state of practice in this field is unsustainable, and results in sub-optimal requirements.

5.3.4 Recommendation

Standardised checklists with a baseline of security requirements should be developed.

To improve the overall security requirements in systems procured by the government, one or more standardised checklists of baseline requirements should be developed. While both the prestudy and the participants in the interviews emphasised the importance of custom security requirements, and a proper cost-benefit-analysis for each security requirement, some security will almost always be needed in modern IT-systems.

There are several ways such a checklist might be implemented, and the actual requirements of such a checklist are outside the scope of this thesis. Based on the feedback from the participants, the checklist should include security areas with specific requirements connected to each area. An example outline for a standardised checklist is given below.

1. Encryption
   - □ All data sent over the internett shall be encrypted.
   - □ Encryption standards used shall not have known defects.
   - □ All private encryption keys shall be stored on a secure air-gapped system.
2. Protection of data and assets
   - □ *Requirement*
3. Operations security
   - □ *Requirement*
4. Authentication of users
   - □ *Requirement*
5. Incident management
   - □ *Requirement*
6. Physical security
   - □ *Requirement*
7. Audit and testing
   - □ *Requirement*
8. Security focus during development
   - □ *Requirement*
9. Organisation security policy
   - □ *Requirement*
10. Compliance
    - □ *Requirement*

It should be noted that only the general format is part of the recommendation. The requirements shown under *encryption* are for illustrative purposes only, and meant to show that each category can have multiple requirements. Security requirements developed for such a checklist must be made by highly experienced security personnel, and reviewed on a regular basis. The categories used in the example are the ones identified as part of the prestudy, and described in Section 3.3. These can be a starting point for the work on such a checklist, as they are derived from known and thoroughly reviewed security standards. The categories were presented to the participants in the questionnaire, as shown in Figure 4.17, and several of the participants found this to be a good set of categories for security requirements.

It is important to emphasise that the goal of standardised checklists is to ensure *some* security, and that systems with especially important assets will always require custom security evaluations. Implementing a set of baseline requirements would ensure that all publicly procured systems live up to a minimum of security. As such, the checklist should be limited in size, focusing on the main security challenges. Having such requirements would also force the suppliers to focus more on security, improving their level of competence.

The main problem with using standardised checklists is the risk that people will stop thinking, and mindlessly follow the list without doing their own risk assessments. The main way to combat this is to increase the security competence for all IT-personnel, ensuring that everyone involved with procurement processes are aware of the limitations of such checklists.

5.4 Resources and competence

Another theme frequently brought up in the interviews was the available resources and competence in the organisation, and the effect on security requirements. There were three areas the availability of resources and competence was especially linked to: The evaluation of bids, performing delivery follow-up, and the general orderer competence in the organisation. The section is concluded with a recommendation for retention and acquisition of security competence in procuring organisations.

5.4.1 Tender evaluation

As the bids from suppliers are received, procurers must evaluate the bids against the evaluation criteria set in the tender. Answers provided by the suppliers must often be compared and rated on a numeric scale. Doing so requires not only knowledge of the tender documents and existing systems, but also an understanding of the security areas in question. In practice, it is not always the case that the required competence is present in the organisations, and the procurers must take the suppliers' words at face value. When asked if the suppliers can gamble on the procurer's lacking competence during bid evaluation, one procurer answered simply: *"Yes, absolutely"*.

Evaluating bids is difficult, and given many security requirements that have detailed descriptions from the suppliers, it becomes expensive and time-consuming. Looking back to Section 5.2.4, having a high number of security requirements implies that each one has little impact on the overall evaluation of the tender. Having to use a lot of time evaluating security requirements, finding that they don't really matter in the big picture, becomes a waste of resources.

Evaluating the answers for the security requirements given is vital in being able to select the most capable supplier. Limiting the number of security requirements makes the tenders easier to evaluate, and increases the importance of each requirement, but might leave out important security features.

5.4.2 Tender follow-up

A closely related subject is the follow-up of the supplier when the system is delivered. Taking delivery of the system includes signing off on its quality and compliance with the terms of the tender. For security requirements, this includes the need to inspect and test the security and make sure it upholds the set standards. In practice, testing the systems was reported as a task given too little priority, something that could easily be exploited by suppliers:

> ”You answer yes to everything, it doesn't matter, because no one will test it anyway, and it might not be testable.” - Supplier

While this was described only as a hypothetical, suppliers brought in to test systems, or take delivery on behalf of customers, reported that it is not unusual to find serious flaws in procured systems. A supplier described a system they helped take delivery of, and the work done by the software developers:

> ”They couldn't have done the simplest vulnerability analysis with the most basic tools of Kali Linux, they had not done it on their own, and that actually frightened me. (...) some of the findings were quite nasty.” - Supplier

Obvious security flaws in delivered software are attributed to the fact that security is difficult, seldom prioritised by procurers, and pushed back to the end of the project. When the deadline approaches, security surfaces as a prime candidate for cutbacks. Without strict follow-up by procurers, the suppliers can get away with delivering sub-standard security features. But the suppliers are not the only ones at fault, as increased follow up of security in software deliveries would send a clear signal that security is front and centre.

5.4.3 Orderer and supplier competence

Many of the challenges described so far in this chapter relate to the competence in the organisations conducting the procurements. Selecting the appropriate security requirements, wording them in a balanced way, using standardised checklists, evaluating bids and performing follow-up all require competence in the field of information security. This highlights the need for internal security competence in the organisations procuring IT-systems. While this might come naturally to the biggest governmental organisations, there are hundreds of smaller organisations and municipalities that probably can not afford, nor attract the required competence.

Although the people interviewed for this study were both qualified and committed to information security, this is most likely not the case in all public organisations in Norway. Suppliers reported that procurers they deal with, in general, lack the necessary security competence and that security requirements are lacking and of poor quality.

It should be noted that many of the procurers that partook in this study reported their dissatisfaction with the security competence of suppliers they have worked with. Several procurers had been forced to educate their suppliers on security, and necessary security measures. The same was true for external competence brought in to aid in the development of tenders:

> "When acquiring larger systems, we used external resources to aid us. And I would have to write the security requirements myself (...). [The suppliers] did not understand anything about the security requirements we attempted to set, not at all, they could not relate to it." - Procurer

It is interesting to note that both suppliers and procurers in the study are dissatisfied with the other side. This is most likely due to the fact that the participants in this study, as mentioned in Section 5.1, are thought to be more security conscious than the average IT-person. Thus, the most likely conclusion is that there is a general lack of knowledge in the field of information security in the Norwegian IT-sector.

5.4.4 Recommendation

Procurers must acquire and/or retain security competence in their organisation, ensuring their ability to evaluate and perform follow-up on security in procured systems.

The procurers' ability to evaluate bids for tender, and to follow up on the system that is delivered has been pointed out as important by many of the participants. If the bids for a tender can not be properly evaluated, there is no way to ensure that the answers provided by the supplier actually fulfils the requirements. Likewise, when the product is delivered, there must be a thorough review of the security in the solution. Performing this evaluation and follow-up on delivery requires specific security competence, which the procurers should ensure is at hand.

It is possible to use external resources to perform these tasks, but when purchasing this service one can run into many of the same obstacles, as the competence of external resources must then be evaluated. As reported by several participants, security knowledge is not always as high in external companies selling this service as expected.

This recommendation becomes even more important in the context of negotiated processes, as recommended in Section 5.2.6. Performing a negotiated process will require the procurers to be able to discuss security requirements with their suppliers, and challenge them on their choices. In combination however, following these recommendations will help procurers to ensure a good foundation for security in systems they acquire.

5.5 Governmental standard terms and conditions (SSA)

The goal of using a semi-structured interview method was for the participants to be able to bring up new themes that had not been considered by the author when preparing for the interviews. One such topic that emerged was the use of the governmental standard terms and conditions (abbreviated *SSA*[2] in Norwegian). The theme was brought up in an interview about halfway through the study, and the theme was added to the interview guide for the remaining interviews. Because of the late addition, only about half of the participants were actively asked about the subject.

The theme was brought up by a supplier:

> "[The SSAs] are in general terrible. (...) The SSAs have ruined a lot by placing a lot of focus on parts of deliveries, but not on totality. And security is god damn not included, I can't remember it being mentioned at all." - Supplier

The procurers asked about this agreed that the SSAs did not provide any help on the matter of security, nor did they present security as an important theme for consideration. Security must be actively included in the agreement by the procurer to be part of the contract. When asked about the SSAs, and how they address security, one procurer said:

[2] Statens Standardavtaler

> "My impression is that [the SSAs] have become relatively thin now, and they make few demands. (...) I think a basic set of [security] requirements could be developed, and used as an attachment to the SSA" - Procurer

It should be noted that several of the participants stated that they had not read the changes implemented in the last revision of the SSAs. As of the newest version, there has been inserted a right to do security audits, a requirement that the supplier ensures adequate information security relating to privacy, as well as a dedicated section on information security. This section reads in its entirety:

> "The Contractor shall implement proportionate measures to address the information security requirements associated with the performance of the deliverables."[43]

This requirement, unfortunately, has many of the weaknesses this thesis has pointed out for security requirements, in that it is vague, does not describe the goal of the security, and is generally easy to claim compliance with. Should procurers rely solely on this requirement, they can not expect good security in their end product.

5.5.1 Recommendation

The governmental standard terms and conditions (SSA) must be revised to include further security focus.

First brought up by one of the participants, the state of SSAs with respect to security needs improvement. Currently, there is little focus on security in the SSA, possibly causing this to be viewed as a less important issue. In the case of organisations with insufficiently competent procurers, or where the balancing between cost, time, functionality and security is especially difficult, the inclusion of better security requirements in the SSAs would help emphasise the importance of security.

As described in Section 5.5, there has recently been a review of the SSAs, resulting in an increased security focus. The SSAs are complex legal documents, and a full analysis of the differences between the current and previous version is not in the scope of this survey. However, based on the change description published by Difi, the changes made in the area of information security appears insufficient compared with the findings of this study. The main addition to information security is too general to provide any support for procurers, other than a reminder of the existence of security issues. While this is a start, it is far from enough to improve today's situation.

5.6 Other topics

In addition to the topics discussed above, there were several topics brought up by some of the participants that merited mention in the results. For these topics, no recommendations are presented, either because the input from the participants was not sufficient for this, or because recommendations can not easily be given. Procurers and suppliers should however note these areas, as they are reported by the participants of this study to impact the security requirements of procured systems.

5.6.1 Security work and methods

Some procurers interviewed use an Information Security Management System (ISMS) to ensure that the work they do on security is structured and formalised. Others approach each system individually, and decide the best process for that particular system. These methods have their own advantages and disadvantages. Not using a formal method makes the procurer vulnerable to skipping important steps in the process, and there is a risk of having to do much of the same work over again for every system. Using an ISMS is not always very well thought through, and blindly following the process and requirements can make the process expensive as one supplier reported:

> ”I remember we got a surprise: You need a secure room, it was to withstand a person using a sledgehammer to get through the walls for a number of minutes, and then you have to start: how thick must the walls be, what must they be made of, and that suddenly increases the cost of the bid. (...) And then you wonder, does the customer know the consequence of us having to fulfil these standards and security requirements.” - Supplier

It appears to be true here as well that a balance of requirements combined with knowledge of security and its implications are important.

The interviews also revealed that many of the participants view security as something more than a technical task, or the lone responsibility of the IT-department. The entire organisation must be involved if security is to succeed, as the access granted to users make them part of the security of the system.

> ”Thinking security can not be something only [the IT-department] does, it is something everyone must do as part of their work.”
> - Procurer

Creating security awareness in the organisation as a whole can also help increase understanding of security requirements in the procurement process.

5.6.2 Certifications

Many suppliers have certifications in the area of information security, and this is also required in order to enter into some tenders. The feedback from both suppliers and procurers are divided on the value of certifications. One procurer said it was an advantage if the suppliers are certified, as it makes it very easy to check if the supplier has the necessary security qualifications. The procurer wanted this to be a basic requirement on a national level, as it would indicate which suppliers were serious on information security. This was countered by another supplier, who made the point that most suppliers who have certifications are certified in secure development, e.g. protecting source code, something that does not necessarily make them skilled at developing secure software. The weaknesses of certifications was exemplified by a third procurer:

> ”(...) we evaluated two suppliers, and one was certified and the other was not certified, but there was no doubt who was better in the area of certification, so them being certified was in a way only a cover, it provided no real value to the customer.” - Procurer

Looking at the weaknesses of certifications, it is interesting to note that several of the procurers reported that requirements for certifications are becoming more common. Being certified thus becomes a competitive advantage and an acceptable cost, as it might be required in later tenders, something that was confirmed by participants.

Certifications should not be treated as a guarantee of a supplier's competence in security, nor the quality of the work they deliver. It however stands to reason that certified suppliers should have a minimum level of security focus, possibly making them better than their uncertified counterparts. However, as certifications are expensive and time-consuming, some suppliers with sufficient security knowledge might choose not to get certified. Procurers should seriously consider if their tenders require a mandatory requirement for security certifications. While such a requirement might make the evaluation of the bids easier, there is a risk of excluding highly qualified suppliers.

5.6.3 Large vs small suppliers

During the interviews, there were several participants who brought up the differences between small and large suppliers.

Large suppliers were reported by procurers to have a far better understanding of the security challenges faced during development of IT-systems.

Additionally, the large suppliers were seen as more able to attract and hire competent security personnel. One procurer made it clear that the smaller companies provided little in terms of security:

> "[We] use 10s or maybe 100 small subcontractors. What is their relation to security? Absolutely none. And why? First and foremost because they don't have the competence, and secondly because they don't have the resources." - Procurer

The large suppliers were however not favourably viewed in their conductions of the procurement process as a whole. Several participants reported that the large suppliers are prone to not answer the tender sufficiently, forcing the procurers to either ask follow-up questions, or in the worst case exclude the suppliers from the competition. One procurer also talked about how suppliers sometimes would not fulfil mandatory requirements in the tender:

> "(...) what I am most surprised about is that the large suppliers make these blunders. And I don't know if it's due to arrogance or carelessness." - Procurer

Another risk associated with using large suppliers, and especially international corporations, is their tendency to either shut down parts of their organisation, or streamline their service in a way that is contrary to the wishes of the customers. A supplier might, for example, choose to relocate their data centres to another country, or shut down the security department and fulfil their contractual obligations by using a subcontractor. This risk is however not mitigated by choosing small suppliers, as they are often bought by larger corporations, and incorporated into their existing organisation.

On the field of information security, it seems that the large suppliers have an advantage in providing more secure products. There is, however, a tendency to mistrust the large suppliers to be able to answer tenders completely, and a fear that the services provided might be changed quickly after coming to an agreement. Going with small suppliers is not likely to improve security, and procurers should rather ensure that they are secured against outsourcing and other changes in the contracts.

5.6.4 Product owners

Another subject brought up by several participants was the competence of the product owner, and how it impacted the IT-departments' ability to ensure security in their products. Product owners in the organisation, be it purchasing departments or project leaders, usually does not have the necessary competence in IT-security, but have to balance the need for security against other factors such as cost and development time. There is limited time to write and evaluate the tenders, and as security is a complex field, it is easily down-prioritised by the product owners.

Several of the participating procurers reported that they were sometimes not brought in on a system acquisition until later in the process, when it was difficult to adapt the system requirements to accommodate security requirements.

> ”One acquires a system for some need the organisation has, without thought for the fact that it is an IT-solution with associated security challenges.” - Procurer

When the IT-department is not running the actual tender process, but rather is one of many actors that contribute to the tender, security can easily become subordinate. Ensuring that security personnel is included in the process early, and giving them the power to implement sufficient security in any system could go a long way in mitigating this challenge.

5.6.5 Prestudy conclusions

The prestudy conducted in the fall of 2015 concluded that the state of security requirements in publicly procured systems was not sufficient, and presented a series of literature recommendations [1].

This thesis has found support for several of the literature recommendations from [1]. Especially the problem in balancing between vague and specific requirements was supported by most of the participants, as discussed in 5.2.1. Participants found this difficult, and reported significant downsides to walking too far in either direction when it comes to the detail level of security requirements.

The lacking use of standards was also brought up as a problem, as there is no common vocabulary or standard requirements suppliers can relate to, or use in order to ease their work on security requirements. In addition, standards could have contributed to a minimum level of security requirements.

The prestudy found that there was a gap between the recommendations for security requirements, and the actual state of practice in the tender documents. This was confirmed by that participants of the study, who reported the state of security requirements as insufficient and with large variations. While the participants seemed to agree that there are both procurers and suppliers who do good work with security requirements, most participants were not happy with the state of the industry in total.

5.7 Limitations

This section describes the limitations of the study. While care has been taken to eliminate sources of errors, avoiding it completely is unlikely. Wide application of the results of the study is mainly limited by the low number of participants and their selection, as described in Section 5.7.1. A priming problem discovered in the survey is presented in Section 5.7.2.

5.7.1 Participant selection

The participants of the study were primarily recruited through the network of Lillian Røstad. As the network consists mainly of security focused people, it is expected that they are not representative of the average IT-operative in Norway. This brings with it both advantages and disadvantages, as described in Section 5.1. The main disadvantage is the lack of representative data on the actual state of security in organisations involved in public procurements in Norway, As the participants are expected to be more than average security focused, their reported security focus is most likely higher than average. The limitations introduced because of this is somewhat offset by the participants' high knowledge of security, and insight into the public procurement process.

Having only 14 participants greatly limits how general the results of the study can be seen as. While statistical significance is not the goal in a qualitative study such as this, it would have been preferable to have a higher number of participants, especially from the supplier side. Participants from suppliers proved much more difficult to recruit, possibly because of the much stricter focus on efficiency and profit in the private sector.

5.7.2 Questionnaire priming

The final questions of the questionnaire ask the participants to rank the areas of security requirements that were identified in the prestudy by importance (Figure 4.18). After this, they are asked to identify the three areas they themselves most commonly write, or see, security requirements for (Figures 4.19 and 4.20). The results point to a correlation between each user's ranking of the areas, and the areas they write requirements in. This would make sense, as an area seen as important would naturally have a greater effort put into it. But the order of the questions might cause the participants to be primed. After ranking the importance of the areas, the participants would either have to answer the top three areas from their ranking, or admit that they write fewer requirements in the most important areas.

Flipping the questions around might have mitigated the problem, though it could have introduced the same priming, just the other way around. As the questions appear on the same page of the survey, there is no way to control the sequence in which the questions were answered, or if the participants revised their answer on question 16 after seeing questions 17 and/or 18. Thus, the results of questions 16, 17 and 18 are not reported in the study. The results for each individual participant was used as a method for starting a conversation with those participants.

Chapter 6

Conclusion and further work

This chapter presents the conclusions of the study of the current state of security requirements in Norwegian public procurements, and provides the findings based on the research questions set forth for the thesis:

RQ1 How is the current state of security requirements in public procurements viewed by procurers and suppliers?

RQ2 What challenges exists when procuring IT-systems, and how does this affect security requirements?

RQ3 What recommendations can be given to improving the current state of security requirements in public procurements?

Section 6.1 describes the findings related to RQ1 and RQ2. Based on RQ3, four areas for which recommendations can be given have been identified and are described in Section 6.2. The presented findings contribute to a better understanding of the areas of research given in the research questions, though further work is required in order to provide definitive answers. Suggestions for further work are presented in Section 6.3.

6.1 State of practice and challenges

The participants of the study reported great variations in the quality of security requirements, and the competence in the industry, as well as numerous challenges in connection with the rules for procurements. The conclusions based on the participants' feedback are presented in this section.

6.1.1 Current state of security requirements in public procurements

In general, the participants were not satisfied with the state of security requirements in Norwegian public procurements. The study found that security requirements generally does not follow the recommendations of the literature, usually by being too vague or too specific. Security is often given low priority, or viewed as too expensive or time consuming by product owners. Security requirements are removed or altered to increase competition for tenders, and there seems to be a general dissatisfaction with the security competence of both procurers and suppliers. Smaller suppliers are seen as less likely to be able to ensure good security, while large suppliers are prone to outsource or change their security work on short notice. An increasing number of procurers are requiring security certifications of their suppliers, but the value of these certifications are disputed.

6.1.2 Security requirement challenges when procuring IT-systems

The procurement process itself adds to the challenges faced by both procurers and suppliers. This study has found that while it is recommended to use negotiated procurement processes to better be able to ensure security in IT-systems, this is not done sufficiently often. The transparency requirements of the procurement process is a challenge to both procurers and suppliers. It results in inadequate security requirements, and poor understanding of these. The governmental standard terms and conditions (SSA) lack security emphasis, and its focus on parts of deliveries, not totality, can hurt IT-security. Standardised requirements are seen as a tool that can help both procurers and suppliers to better ensure high security in procured systems. Both procurers and suppliers agree that there is a need for procurers to have a certain level of security competence in order to be able to use standardised checklists, evaluate bids, and perform checks and follow-up of the final product.

6.2 Recommendations

This section describes the findings related to RQ3, and presents the recommendations given in this thesis. The recommendations are outlined in Table 6.1, and described briefly below.

Implementation of the recommendations should be done by experienced security operatives, with a deep understanding of both IT-security and the public procurement process.

Table 6.1: Recommendations for improvements in Norwegian Public Procurements

#	Recommendation
1	Use negotiated processes
2	Develop standardised checklists for security requirements
3	Procurers must retain security competence
4	Improve security focus in the governmental standard terms and conditions (SSA)

6.2.1 Use negotiated processes

Recommendation:
It is highly recommended that procurers shift tenders for IT-systems to negotiated processes, especially for systems that are security critical.

As many of the challenges faced by both procurers and suppliers in the procurement process is due to the rigid and inflexible nature of the procurement regulations, a shift towards processes which open for dialogue is recommended. Procurers and suppliers both advised the switch away from standard open competitions to ensure that security requirements could be fulfilled in the best possible way. Negotiated processes are more expensive, and require procurers to ensure fair treatment of all suppliers. Nevertheless, the advantages are seen by participants to outweigh these drawbacks.

6.2.2 Develop standardised checklists for security requirements

Recommendation:
Standardised checklists with a baseline of security requirements should be developed.

The prestudy found a lack of satisfying security requirements in many of the studied tenders, a view supported by the participants of this study. As writing security requirements is a complex task, requiring a high level of competence, participants would like to see the development of one or more standardised checklists for security requirements. Several possible designs were suggested, with a list of baseline requirements being most popular.

Such lists would enable organisations that currently have no, or very limited, security requirements to gain a minimum of security. A security requirement checklist must be developed by seasoned security operatives, and kept up to date.

6.2.3 Procurers must retain security competence

Recommendation:
Procurers must acquire and/or retain security competence in their organisation, ensuring their ability to evaluate and perform follow-up on security in procured systems.

Evaluating the bids for a tender, and performing follow-up when taking delivery of a system, requires security competence. The participants reported that many organisations were not capable of performing these tasks satisfactory, making it possible for suppliers to get away with less security than contractually specified. Security requirements given in requirement specifications must be followed up when the system is delivered. To accomplish this, procurers must have security competence internally in their organisation, and this competence must be retained.

6.2.4 Improve security focus in the governmental standard terms and conditions (SSA)

Recommendation:
The governmental standard terms and conditions (SSA) must be revised to include further security focus.

First brought up by one of the participants, the SSAs are not seen as contributing enough to security, and are possibly hurting it. The main objection to the SSAs by the participants was the lack of specific requirements on security, and how they shift focus from totality to individual parts of delivery. While some changes have been made to the SSAs lately to address security concerns, these are prone to many of the mistakes identified in the prestudy. The SSAs should develop a clear focus on security, a work that should be seen in connection with the recommendation of standardised checklists of security requirement.

6.3 Further work

This thesis has presented the current state of security requirements in Norwegian public procurements, an interview study with 14 security operatives, and given four main recommendations for improvement of security requirements. This section presents recommendations for further work on the subject and surrounding areas of research.

6.3.1 Development of checklists

Section 6.2.2 recommends the development of standardised checklists of baseline security requirements. While an outline of possible categories is presented in Section 5.3.4, the actual requirements are outside the scope of the thesis. These should be developed by experienced security personnel, with a high technical understanding, and practical experience working in the industry. There is a need for an empirical basis for this work, it can not be done as an academic exercise, but must rather be done by the people working with security requirements in public procurements as part of their job. To ensure broad adaptation and make inclusion into the governmental standard terms and conditions possible, the work must be in collaboration with, or at least approved by, the Agency for Public Management and eGovernment - Difi.

6.3.2 Extended study

The combined results of the prestudy and this thesis point to a state of practice in security requirements that does not support high security. The results are mainly limited by the size of the data material used, with 29 tenders analysed, and 14 participants interviewed.

An extended study of the document analysis, performed on several hundred tender documents could gain the needed statistical significance to find correlations between the quality of security requirements and cost, organisation type, organisation size and so on. This probably needs to be supported by some kind of automatic evaluation of security requirements, building on the work of [44].

Likewise, a larger number of participants to interview would enable more general conclusions to be drawn. Here, the focus should be to bring in more suppliers, and to enlist participants from a statistical representative selection of organisations.

6.3.3 Case study

Analysing tender documents, and interviewing selected security operatives will only enable a glimpse into the work done to write and fulfil security requirements. While difficult, a set of case studies on how this process is done could potentially greatly increase the understanding of security requirement work in public procurements. As described in Section 4.4.2, there is a risk of the scientist altering the behaviour of participants, an effect difficult to circumvent.

6.3.4 International studies

The research of this thesis has been in the context of the Norwegian procurement rules and IT-industry. As the laws and regulations for procurements are the same in Norway as in the rest of the European Economic Area (EEA) and the European Union (EU), there should not be huge discrepancies with other countries within these areas. However, as business culture and other factors vary across countries, similar research from other EEA/EU-countries would be interesting. In addition, performing similar studies in countries outside the EEA/EU would provide an opportunity to understand how the procurement process affects security requirements, compared with countries that have either stronger or weaker procurement laws.

Bibliography

[1] H. K. Henriksen, “Security Requirements in Norwegian Public Procurement,” dec 2015, unpublished prestuy, conducted as part of master study at NTNU.

[2] (2006, apr) Forskrift om offentlige anskaffelser - §2-1 (2). [Online]. Available: http://lovdata.no/forskrift/2006-04-07-402/%C2%A72-1

[3] “Forskrift om offentlige anskaffelser,” apr 2006. [Online]. Available: https://lovdata.no/dokument/SF/forskrift/2006-04-07-402

[4] S. Lauesen, “Cots tenders and integration requirements,” *Requirements Engineering*, vol. 11, no. 2, pp. 111–122, 2006. [Online]. Available: http://dx.doi.org/10.1007/s00766-005-0022-5

[5] ——, “Experiences from a tender process,” in *Proceedings of REFSQ’04*, 2004, pp. 29–46.

[6] C. E. Moe and T. Päivärinta, “Challenges in information systems procurement in the public sector,” *Electronic Journal of e-Government*, vol. 11, no. 1, 2013.

[7] “Lov om behandling av personopplysninger - §31,” apr 2000. [Online]. Available: https://lovdata.no/dokument/NL/lov/2000-04-14-31/

[8] K. V. Thai, “Public procurement re-examined,” *Journal of public procurement*, vol. 1, no. 1, pp. 9–50, 2001.

[9] W. Wensink and J. Vet, “Identifying and reducing corruption in public procurement in the eu,” *Brussels: PwC EU Services*, 2013.

[10] “Lov om offentlige anskaffelser,” jul 1997. [Online]. Available: https://lovdata.no/dokument/NL/lov/1999-07-16-69

[11] OECD, "Collusion and corruption in public procurement," pp. 283–287, 2010. [Online]. Available: http://www.oecd.org/competition/cartels/46235884.pdf

[12] DIFI. (2015, oct) Anbudskonkurranse - åpen og begrenset. [Online]. Available: http://www.anskaffelser.no/anskaffelsesfaglige-temaer/anskaffelsesprosedyrer/anbudskonkurranse-apen-og-begrenset

[13] D. for forvaltning og IKT. (2015, oct) Konkurranse med forhandling. [Online]. Available: http://www.anskaffelser.no/anskaffelsesfaglige-temaer/anskaffelsesprosedyrer/konkurranse-med-forhandlinger

[14] (2006, apr) Forskrift om offentlige anskaffelser - §14-2. [Online]. Available: http://lovdata.no/forskrift/2006-04-07-402/%C2%A714-2

[15] DIFI. (2015, oct) Konkurransepreget dialog. [Online]. Available: http://www.anskaffelser.no/anskaffelsesfaglige-temaer/anskaffelsesprosedyrer/konkurransepreget-dialog

[16] ——. (2015, Nov) Konkurransepreget dialog ved innovative anskaffelser. [Online]. Available: http://www.anskaffelser.no/prosess/innovasjon/innovasjon-steg-steg/gjennomfore-konkurranse/valg-av-prosedyre/konkurransepreget

[17] ——. (2015, Nov) Anskaffelsesprosessen. [Online]. Available: http://www.anskaffelser.no/prosess/anskaffelsesprosessen

[18] (2015, Nov) Avgjorte saker. KOFA. [Online]. Available: http://www.kofa.no/no/Avgjorte-saker/

[19] S. Renault, Ó. Méndez Bonilla, J. Franch Gutiérrez, M. C. Quer Bosor *et al.*, "A pattern-based method for building requirements documents in call-for-tender processes," 2009.

[20] B. Paech, R. Heinrich, G. Zorn-Pauli, A. Jung, and S. Tadjiky, "Answering a request for proposal – challenges and proposed solutions," in *Requirements Engineering: Foundation for Software Quality*, ser. Lecture Notes in Computer Science, B. Regnell and D. Damian, Eds. Springer Berlin Heidelberg, 2012, vol. 7195, pp. 16–29. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-28714-5_2

[21] (2012, Jan) Her er it-norges 100 mektigste. Computer World. [Online]. Available: http://www.cw.no/artikkel/offentlig-sektor/her-it-norges-100-mektigste

[22] "Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)," may 2006.

[23] I. Tondel, M. Jaatun, and P. Meland, "Security requirements for the rest of us: A survey," *Software, IEEE*, vol. 25, no. 1, pp. 20–27, Jan 2008.

[24] ISO, "Information technology— security techniques — information security management systems — requirements," International Organization for Standardization, Geneva, Switzerland, ISO 27002-2012 2:2013, 2013.

[25] (2015, oct) Common criteria. [Online]. Available: https://www.commoncriteriaportal.org/

[26] PCI Security Standards Council, "Requirements and security assessment procedures - version 3.1," 2015.

[27] C. Robson, *Real world research: A resource for social scientists and practitioner-researchers.* Blackwell Oxford, 2011.

[28] M. Galesic and M. Bosnjak, "Effects of questionnaire length on participation and indicators of response quality in a web survey," *Public opinion quarterly*, vol. 73, no. 2, pp. 349–360, 2009.

[29] P. Marsden and J. Wright, *Handbook of Survey Research*, ser. EBL-Schweitzer. Emerald, 2010. [Online]. Available: https://books.google.no/books?id=mMPDPXpTP-0C

[30] M. D. Myers and M. Newman, "The qualitative interview in {IS} research: Examining the craft," *Information and Organization*, vol. 17, no. 1, pp. 2 – 26, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1471772706000352

[31] J. Ritchie, J. Lewis, C. M. Nicholls, R. Ormston *et al.*, *Qualitative research practice: A guide for social science students and researchers*, 1st ed. Sage, 2003.

[32] S. Hannabuss, "Research interviews," *New Library World*, vol. 97, no. 5, pp. 22–30, 1996. [Online]. Available: http://dx.doi.org/10.1108/03074809610122881

[33] O. Doody and M. Noonan, "Preparing and conducting interviews to collect data," *Nurse Researcher*, vol. 20, no. 5, pp. 28–32, 2013.

[34] I. S. R. Herbert J. Rubin, *Qualitative Interviewing (2nd ed.): The Art of Hearing Data*, 2nd ed. SAGE Publications, Inc., 2005. [Online]. Available: http://dx.doi.org/10.4135/9781452226651

[35] J. Ritchie, J. Lewis, C. M. Nicholls, R. Ormston *et al.*, *Qualitative research practice: A guide for social science students and researchers*, 2nd ed. Sage, 2013.

[36] K. KELLEY, B. CLARK, V. BROWN, and J. SITZIA, "Good practice in the conduct and reporting of survey research," *International Journal for Quality in Health Care*, vol. 15, no. 3, pp. 261–266, 2003. [Online]. Available: http://intqhc.oxfordjournals.org/content/15/3/261

[37] M. Coughlan, P. Cronin, and F. Ryan, "Survey research: Process and limitations." *International Journal of Therapy & Rehabilitation*, vol. 16, no. 1, pp. 9 – 15, 2009. [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=asx&AN=36258303&site=eds-live

[38] Research Consortium on Educational Outcomes & Poverty. (2016, may) Prompts, probes and encouragement. [Online]. Available: http://oer.educ.cam.ac.uk/w/images/b/be/RECOUP_Semi-structured_interviews_prompts_and_probes.pdf

[39] N. King, "Qualitative methods in organizational research: A practical guide," *The Qualitative Research Interview*, p. 17, 1994.

[40] K. L. Easton, J. F. McComish, and R. Greenberg, "Avoiding common pitfalls in qualitative data collection and transcription," *Qualitative health research*, vol. 10, no. 5, pp. 703–707, 2000.

[41] G. J. Skulmoski, F. T. Hartman, and J. Krahn, "The delphi method for graduate research," *Journal of Information Technology Education: Research*, vol. 6, 2007. [Online]. Available: http://www.jite.org/documents/Vol6/JITEv6p001-021Skulmoski212.pdf

[42] D. G. Firesmith and F. Consulting, "Engineering security requirements," *Journal of Object Technology*, vol. 2, pp. 53–68, 2003.

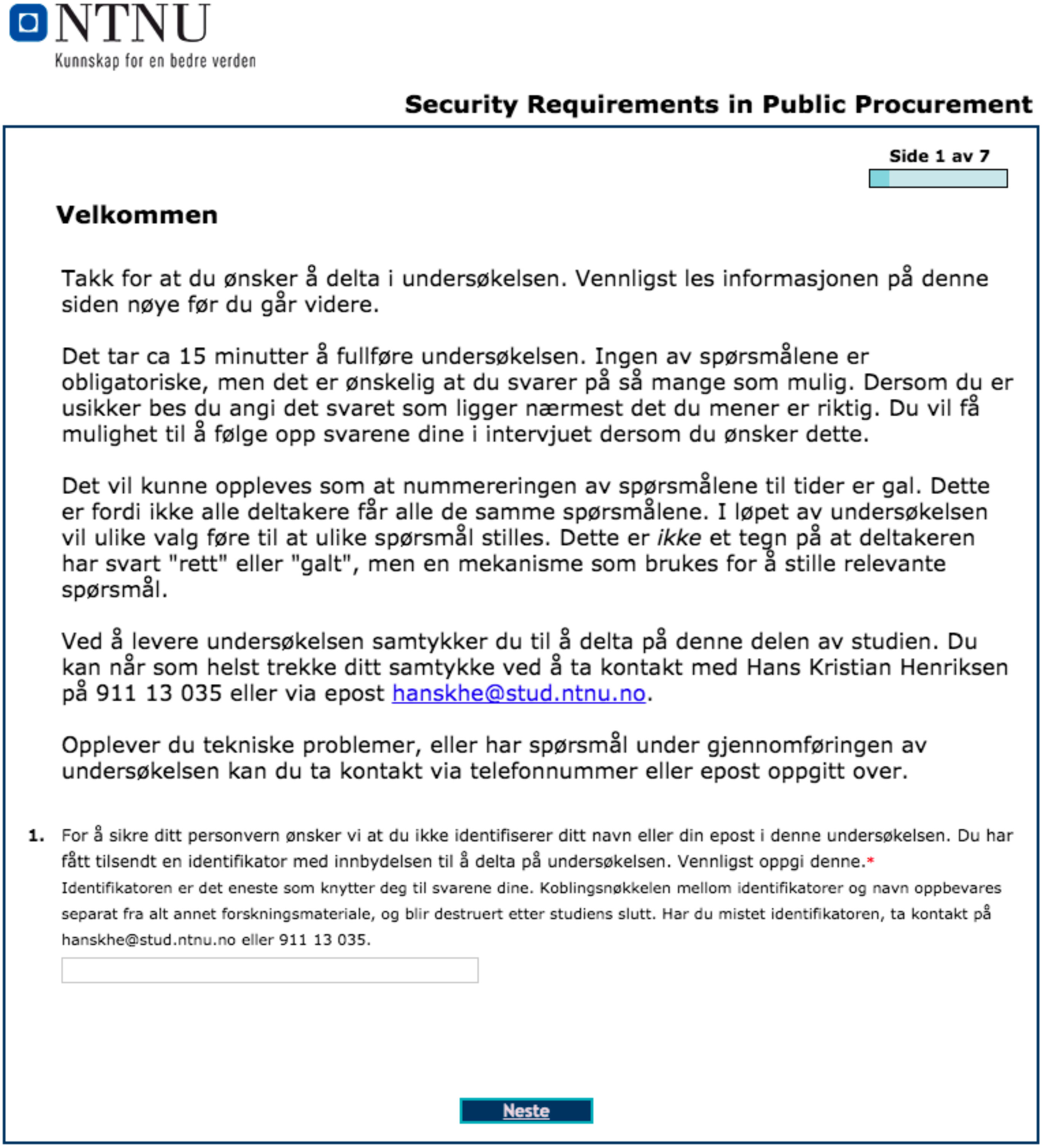
[43] DIFI. (2016, may) Endringer i ssa-t - 2015. [Online]. Available: http://www.anskaffelser.no/verktoy/utviklings-og-tilpasningsavtalen-ssa-t

[44] G. Lami, S. Gnesi, F. Fabbrini, M. Fusani, and G. Trentanni, "An automatic tool for the analysis of natural language requirements," *Informe técnico, CNR Information Science and Technology Institute, Pisa, Italia, Setiembre*, 2004.

Appendix A

Questionnaire

This appendix includes the questionnaire sent to the participants. It is presented here in the exact form the participants saw when answering it. The survey is presented in its original Norwegian.



NTNU
Kunnskap for en bedre verden

Security Requirements in Public Procurement

Side 1 av 7

Velkommen

Takk for at du ønsker å delta i undersøkelsen. Vennligst les informasjonen på denne siden nøye før du går videre.

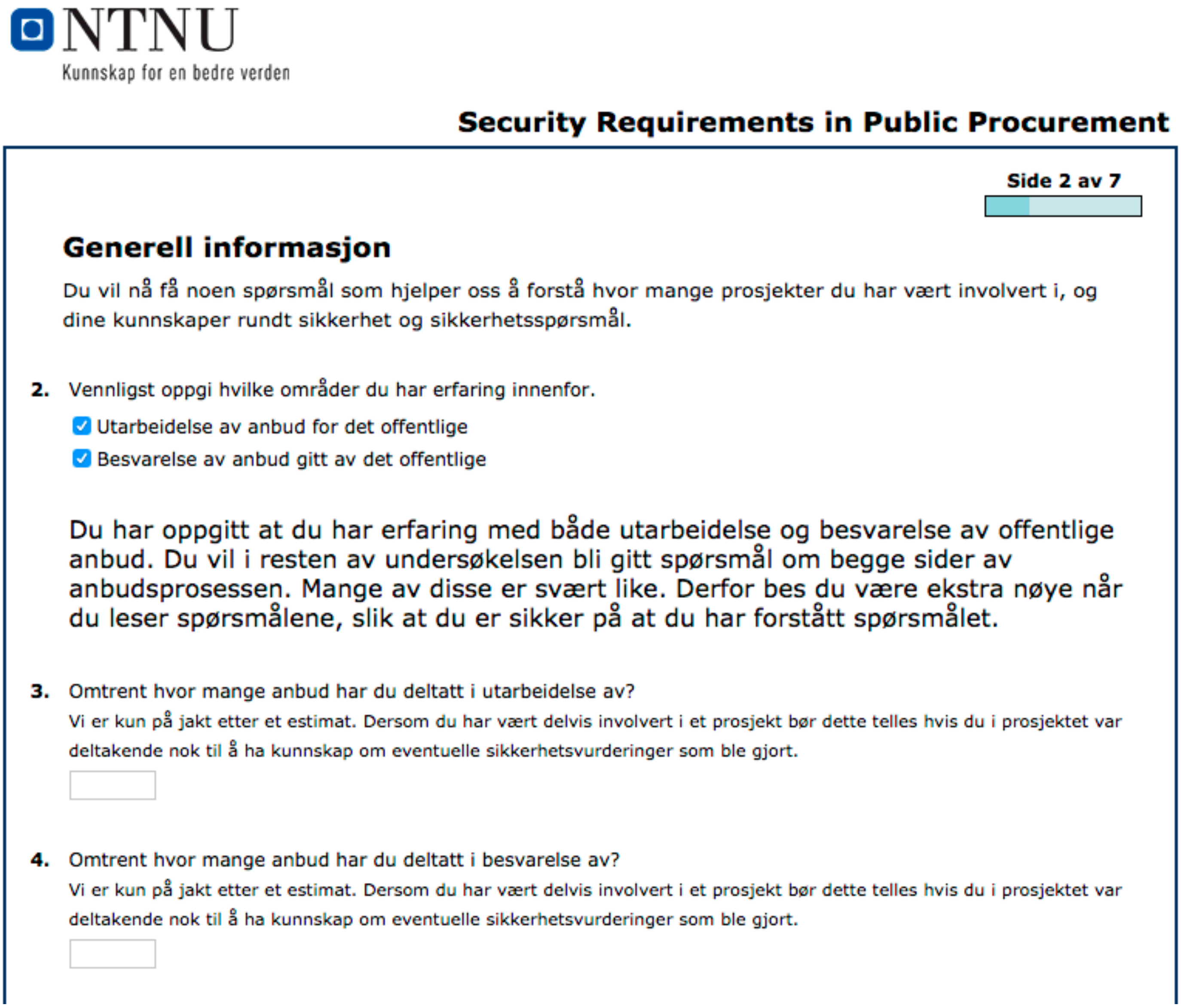
Det tar ca 15 minutter å fullføre undersøkelsen. Ingen av spørsmålene er obligatoriske, men det er ønskelig at du svarer på så mange som mulig. Dersom du er usikker bes du angi det svaret som ligger nærmest det du mener er riktig. Du vil få mulighet til å følge opp svarene dine i intervjuet dersom du ønsker dette.

Det vil kunne oppleves som at nummereringen av spørsmålene til tider er gal. Dette er fordi ikke alle deltakere får alle de samme spørsmålene. I løpet av undersøkelsen vil ulike valg føre til at ulike spørsmål stilles. Dette er *ikke* et tegn på at deltakeren har svart "rett" eller "galt", men en mekanisme som brukes for å stille relevante spørsmål.

Ved å levere undersøkelsen samtykker du til å delta på denne delen av studien. Du kan når som helst trekke ditt samtykke ved å ta kontakt med Hans Kristian Henriksen på 911 13 035 eller via epost hanskhe@stud.ntnu.no.

Opplever du tekniske problemer, eller har spørsmål under gjennomføringen av undersøkelsen kan du ta kontakt via telefonnummer eller epost oppgitt over.

1. For å sikre ditt personvern ønsker vi at du ikke identifiserer ditt navn eller din epost i denne undersøkelsen. Du har fått tilsendt en identifikator med innbydelsen til å delta på undersøkelsen. Vennligst oppgi denne.*
Identifikatoren er det eneste som knytter deg til svarene dine. Koblingsnøkkelen mellom identifikatorer og navn oppbevares separat fra alt annet forskningsmateriale, og blir destruert etter studiens slutt. Har du mistet identifikatoren, ta kontakt på hanskhe@stud.ntnu.no eller 911 13 035.



NTNU

Kunnskap for en bedre verden

Security Requirements in Public Procurement

Side 2 av 7

Generell informasjon

Du vil nå få noen spørsmål som hjelper oss å forstå hvor mange prosjekter du har vært involvert i, og dine kunnskaper rundt sikkerhet og sikkerhetsspørsmål.

2. Vennligst oppgi hvilke områder du har erfaring innenfor.

☑ Utarbeidelse av anbud for det offentlige

☑ Besvarelse av anbud gitt av det offentlige

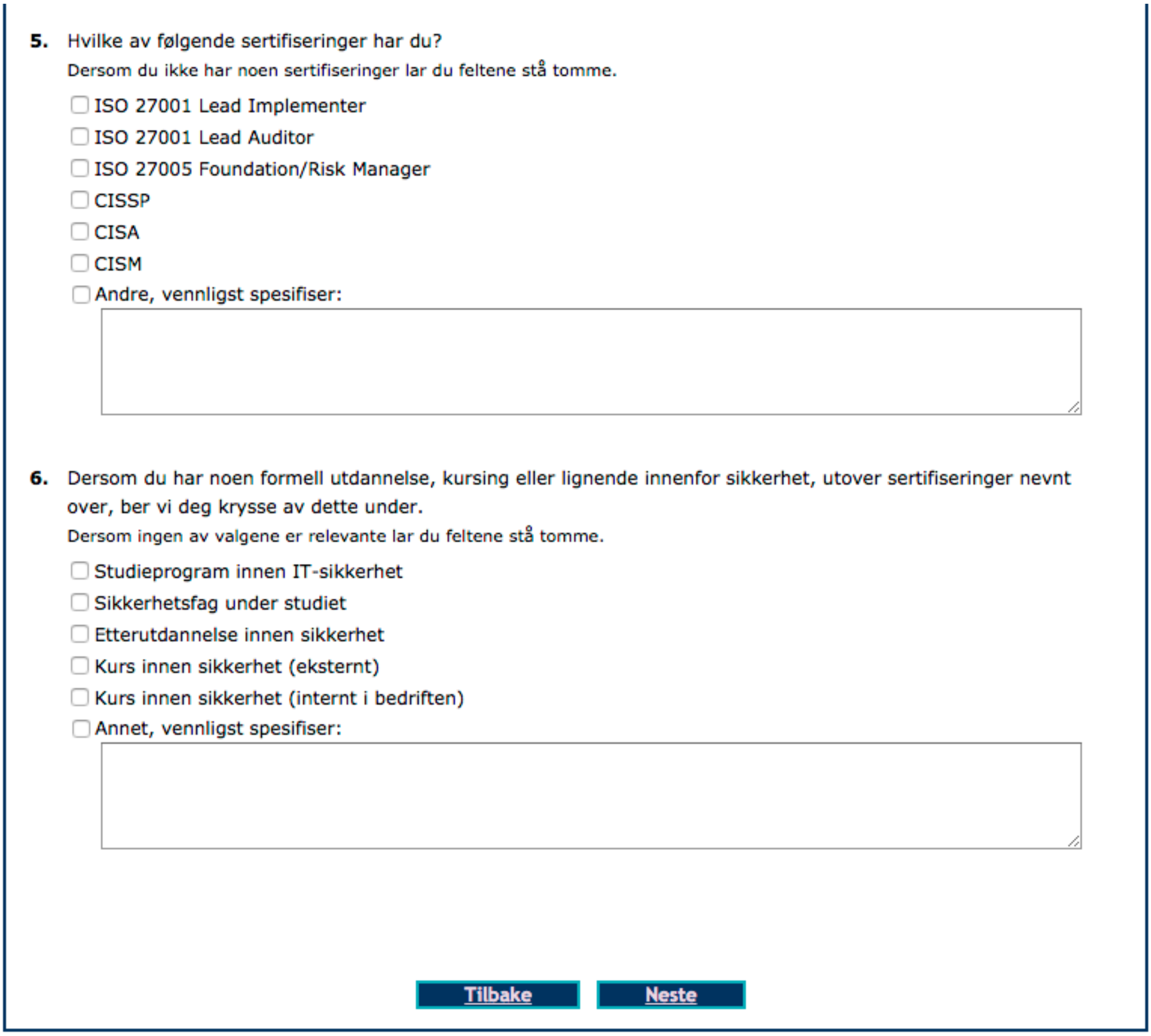
Du har oppgitt at du har erfaring med både utarbeidelse og besvarelse av offentlige anbud. Du vil i resten av undersøkelsen bli gitt spørsmål om begge sider av anbudsprosessen. Mange av disse er svært like. Derfor bes du være ekstra nøye når du leser spørsmålene, slik at du er sikker på at du har forstått spørsmålet.

3. Omtrent hvor mange anbud har du deltatt i utarbeidelse av?

Vi er kun på jakt etter et estimat. Dersom du har vært delvis involvert i et prosjekt bør dette telles hvis du i prosjektet var deltakende nok til å ha kunnskap om eventuelle sikkerhetsvurderinger som ble gjort.

4. Omtrent hvor mange anbud har du deltatt i besvarelse av?

Vi er kun på jakt etter et estimat. Dersom du har vært delvis involvert i et prosjekt bør dette telles hvis du i prosjektet var deltakende nok til å ha kunnskap om eventuelle sikkerhetsvurderinger som ble gjort.



5. Hvilke av følgende sertifiseringer har du?

Dersom du ikke har noen sertifiseringer lar du feltene stå tomme.

□ ISO 27001 Lead Implementer

□ ISO 27001 Lead Auditor

□ ISO 27005 Foundation/Risk Manager

□ CISSP

□ CISA

□ CISM

□ Andre, vennligst spesifiser:

6. Dersom du har noen formell utdannelse, kursing eller lignende innenfor sikkerhet, utover sertifiseringer nevnt over, ber vi deg krysse av dette under.

Dersom ingen av valgene er relevante lar du feltene stå tomme.

□ Studieprogram innen IT-sikkerhet

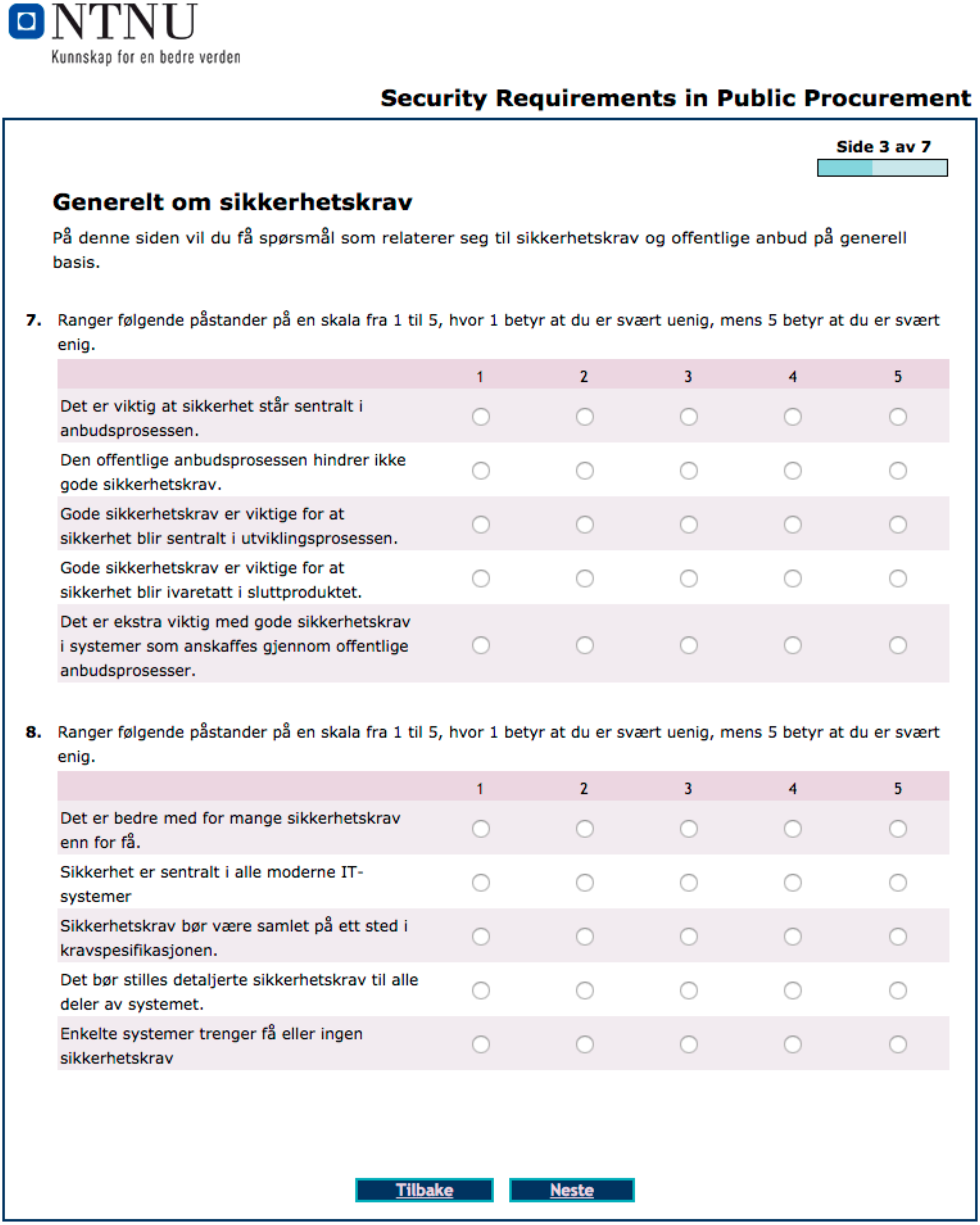
□ Sikkerhetsfag under studiet

□ Etterutdannelse innen sikkerhet

□ Kurs innen sikkerhet (eksternt)

□ Kurs innen sikkerhet (internt i bedriften)

□ Annet, vennligst spesifiser:



Security Requirements in Public Procurement

Side 3 av 7

Generelt om sikkerhetskrav

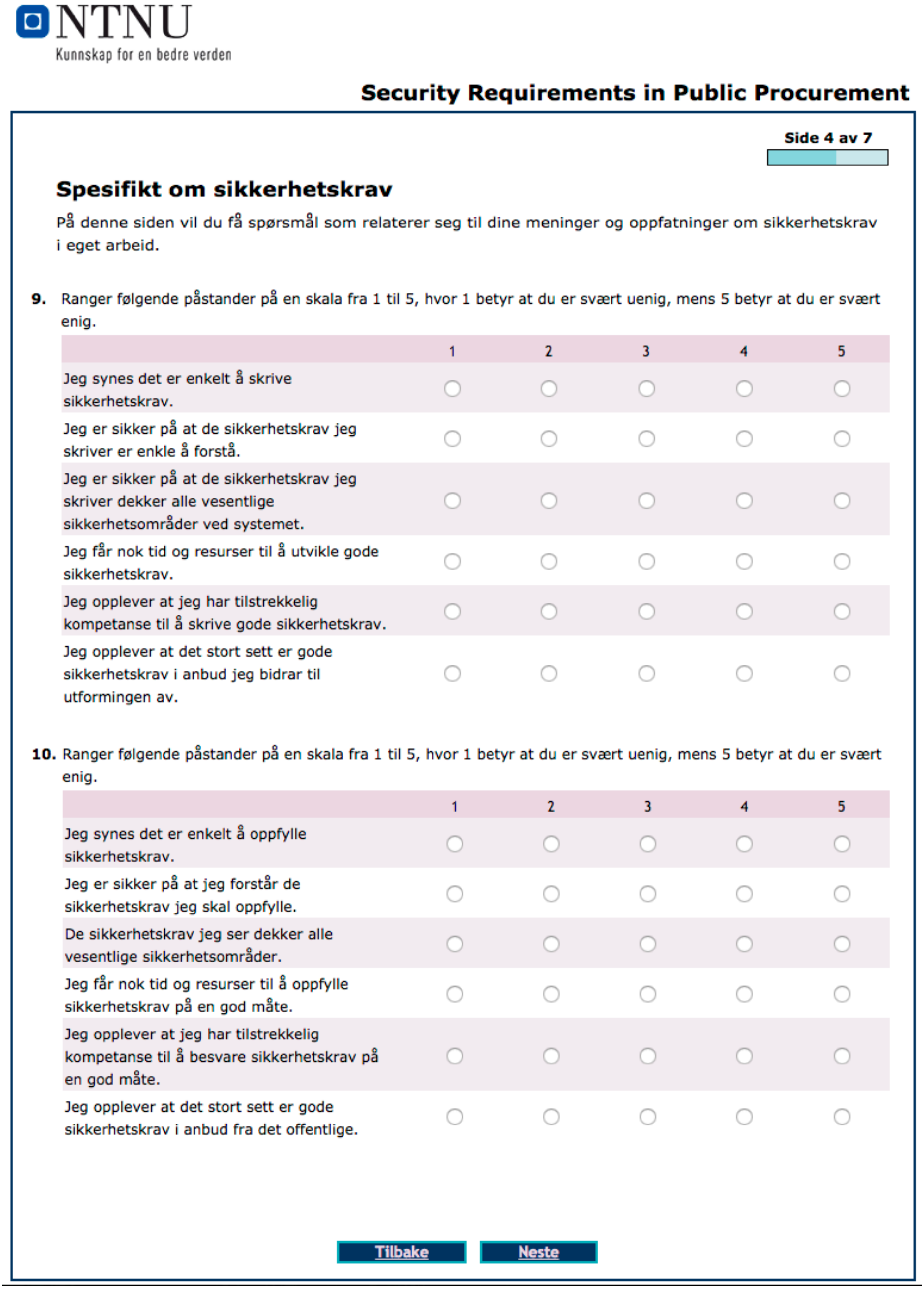
På denne siden vil du få spørsmål som relaterer seg til sikkerhetskrav og offentlige anbud på generell basis.

7. Ranger følgende påstander på en skala fra 1 til 5, hvor 1 betyr at du er svært uenig, mens 5 betyr at du er svært enig.

	1	2	3	4	5
Det er viktig at sikkerhet står sentralt i anbudsprosessen.	○	○	○	○	○
Den offentlige anbudsprosessen hindrer ikke gode sikkerhetskrav.	○	○	○	○	○
Gode sikkerhetskrav er viktige for at sikkerhet blir sentralt i utviklingsprosessen.	○	○	○	○	○
Gode sikkerhetskrav er viktige for at sikkerhet blir ivaretatt i sluttproduktet.	○	○	○	○	○
Det er ekstra viktig med gode sikkerhetskrav i systemer som anskaffes gjennom offentlige anbudsprosesser.	○	○	○	○	○

8. Ranger følgende påstander på en skala fra 1 til 5, hvor 1 betyr at du er svært uenig, mens 5 betyr at du er svært enig.

	1	2	3	4	5
Det er bedre med for mange sikkerhetskrav enn for få.	○	○	○	○	○
Sikkerhet er sentralt i alle moderne IT-systemer	○	○	○	○	○
Sikkerhetskrav bør være samlet på ett sted i kravspesifikasjonen.	○	○	○	○	○
Det bør stilles detaljerte sikkerhetskrav til alle deler av systemet.	○	○	○	○	○
Enkelte systemer trenger få eller ingen sikkerhetskrav	○	○	○	○	○



NTNU
Kunnskap for en bedre verden

Security Requirements in Public Procurement

Side 4 av 7

Spesifikt om sikkerhetskrav

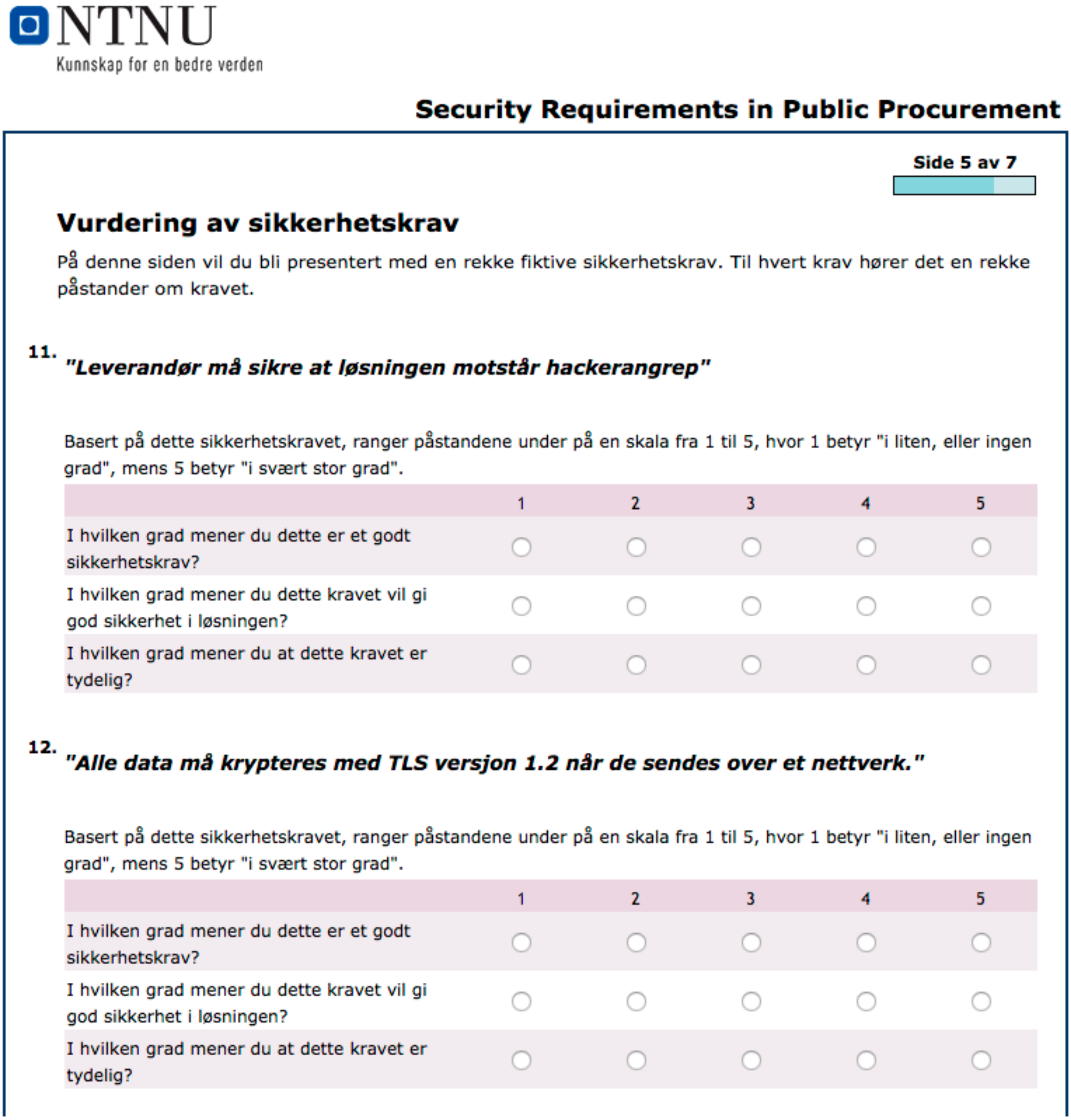
På denne siden vil du få spørsmål som relaterer seg til dine meninger og oppfatninger om sikkerhetskrav i eget arbeid.

9. Ranger følgende påstander på en skala fra 1 til 5, hvor 1 betyr at du er svært uenig, mens 5 betyr at du er svært enig.

	1	2	3	4	5
Jeg synes det er enkelt å skrive sikkerhetskrav.	○	○	○	○	○
Jeg er sikker på at de sikkerhetskrav jeg skriver er enkle å forstå.	○	○	○	○	○
Jeg er sikker på at de sikkerhetskrav jeg skriver dekker alle vesentlige sikkerhetsområder ved systemet.	○	○	○	○	○
Jeg får nok tid og resurser til å utvikle gode sikkerhetskrav.	○	○	○	○	○
Jeg opplever at jeg har tilstrekkelig kompetanse til å skrive gode sikkerhetskrav.	○	○	○	○	○
Jeg opplever at det stort sett er gode sikkerhetskrav i anbud jeg bidrar til utformingen av.	○	○	○	○	○

10. Ranger følgende påstander på en skala fra 1 til 5, hvor 1 betyr at du er svært uenig, mens 5 betyr at du er svært enig.

	1	2	3	4	5
Jeg synes det er enkelt å oppfylle sikkerhetskrav.	○	○	○	○	○
Jeg er sikker på at jeg forstår de sikkerhetskrav jeg skal oppfylle.	○	○	○	○	○
De sikkerhetskrav jeg ser dekker alle vesentlige sikkerhetsområder.	○	○	○	○	○
Jeg får nok tid og resurser til å oppfylle sikkerhetskrav på en god måte.	○	○	○	○	○
Jeg opplever at jeg har tilstrekkelig kompetanse til å besvare sikkerhetskrav på en god måte.	○	○	○	○	○
Jeg opplever at det stort sett er gode sikkerhetskrav i anbud fra det offentlige.	○	○	○	○	○



NTNU
Kunnskap for en bedre verden

Security Requirements in Public Procurement

Side 5 av 7

Vurdering av sikkerhetskrav

På denne siden vil du bli presentert med en rekke fiktive sikkerhetskrav. Til hvert krav hører det en rekke påstander om kravet.

11. ***"Leverandør må sikre at løsningen motstår hackerangrep"***

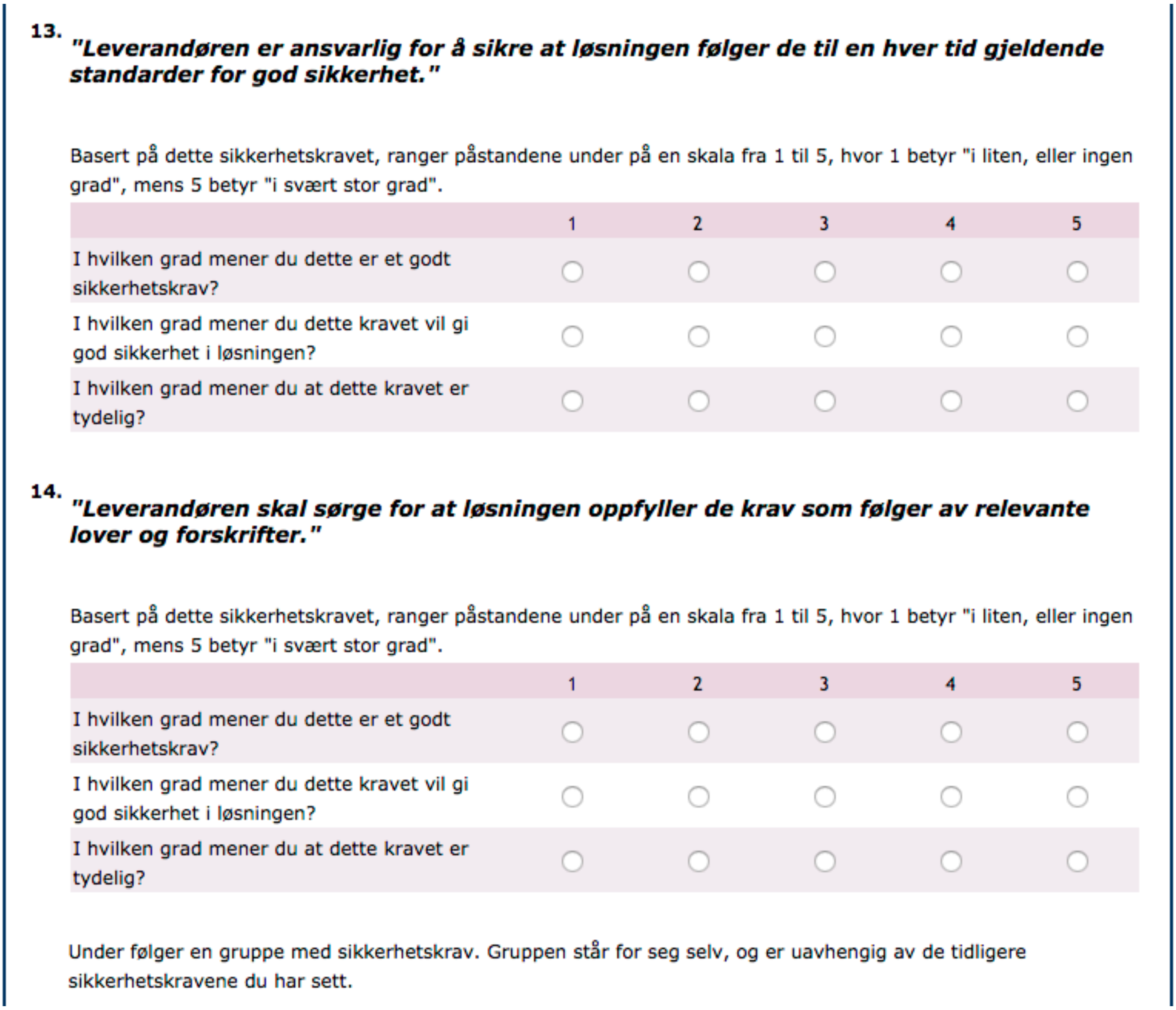
Basert på dette sikkerhetskravet, ranger påstandene under på en skala fra 1 til 5, hvor 1 betyr "i liten, eller ingen grad", mens 5 betyr "i svært stor grad".

	1	2	3	4	5
I hvilken grad mener du dette er et godt sikkerhetskrav?	○	○	○	○	○
I hvilken grad mener du dette kravet vil gi god sikkerhet i løsningen?	○	○	○	○	○
I hvilken grad mener du at dette kravet er tydelig?	○	○	○	○	○

12. ***"Alle data må krypteres med TLS versjon 1.2 når de sendes over et nettverk."***

Basert på dette sikkerhetskravet, ranger påstandene under på en skala fra 1 til 5, hvor 1 betyr "i liten, eller ingen grad", mens 5 betyr "i svært stor grad".

	1	2	3	4	5
I hvilken grad mener du dette er et godt sikkerhetskrav?	○	○	○	○	○
I hvilken grad mener du dette kravet vil gi god sikkerhet i løsningen?	○	○	○	○	○
I hvilken grad mener du at dette kravet er tydelig?	○	○	○	○	○



13. ***"Leverandøren er ansvarlig for å sikre at løsningen følger de til en hver tid gjeldende standarder for god sikkerhet."***

Basert på dette sikkerhetskravet, ranger påstandene under på en skala fra 1 til 5, hvor 1 betyr "i liten, eller ingen grad", mens 5 betyr "i svært stor grad".

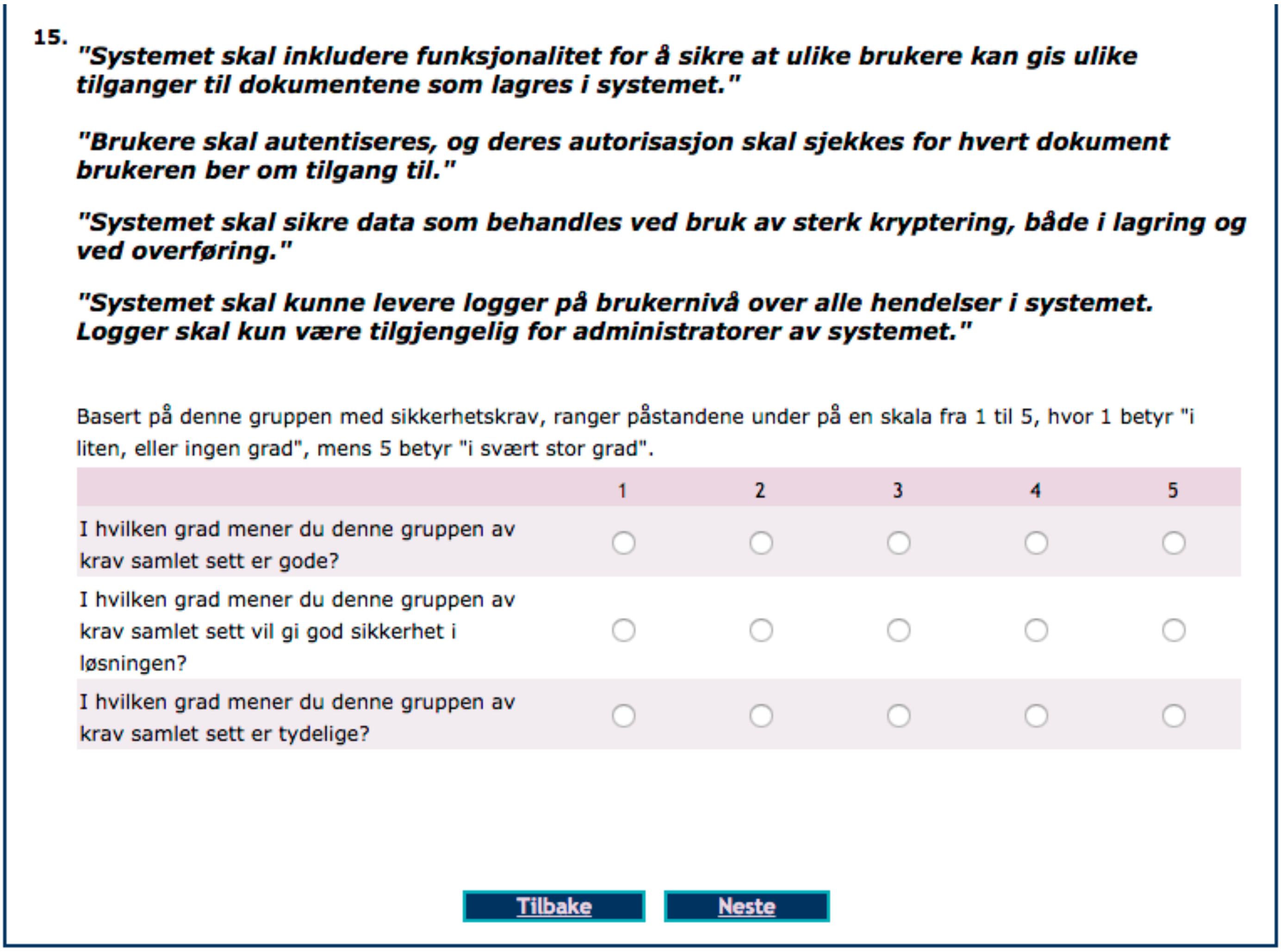
	1	2	3	4	5
I hvilken grad mener du dette er et godt sikkerhetskrav?	○	○	○	○	○
I hvilken grad mener du dette kravet vil gi god sikkerhet i løsningen?	○	○	○	○	○
I hvilken grad mener du at dette kravet er tydelig?	○	○	○	○	○

14. ***"Leverandøren skal sørge for at løsningen oppfyller de krav som følger av relevante lover og forskrifter."***

Basert på dette sikkerhetskravet, ranger påstandene under på en skala fra 1 til 5, hvor 1 betyr "i liten, eller ingen grad", mens 5 betyr "i svært stor grad".

	1	2	3	4	5
I hvilken grad mener du dette er et godt sikkerhetskrav?	○	○	○	○	○
I hvilken grad mener du dette kravet vil gi god sikkerhet i løsningen?	○	○	○	○	○
I hvilken grad mener du at dette kravet er tydelig?	○	○	○	○	○

Under følger en gruppe med sikkerhetskrav. Gruppen står for seg selv, og er uavhengig av de tidligere sikkerhetskravene du har sett.



15. ***"Systemet skal inkludere funksjonalitet for å sikre at ulike brukere kan gis ulike tilganger til dokumentene som lagres i systemet."***

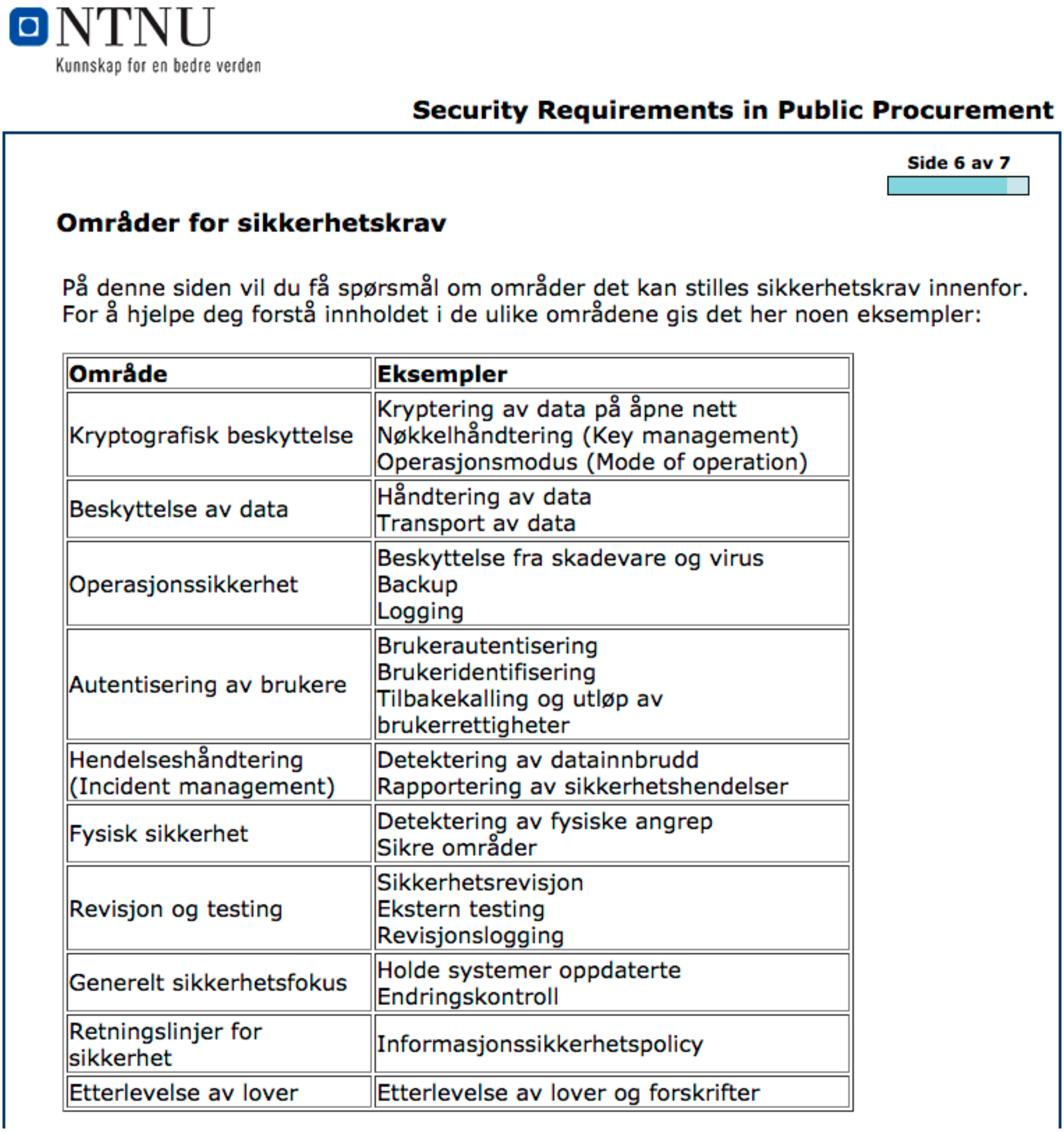
"Brukere skal autentiseres, og deres autorisasjon skal sjekkes for hvert dokument brukeren ber om tilgang til."

"Systemet skal sikre data som behandles ved bruk av sterk kryptering, både i lagring og ved overføring."

"Systemet skal kunne levere logger på brukernivå over alle hendelser i systemet. Logger skal kun være tilgjengelig for administratorer av systemet."

Basert på denne gruppen med sikkerhetskrav, ranger påstandene under på en skala fra 1 til 5, hvor 1 betyr "i liten, eller ingen grad", mens 5 betyr "i svært stor grad".

	1	2	3	4	5
I hvilken grad mener du denne gruppen av krav samlet sett er gode?	○	○	○	○	○
I hvilken grad mener du denne gruppen av krav samlet sett vil gi god sikkerhet i løsningen?	○	○	○	○	○
I hvilken grad mener du denne gruppen av krav samlet sett er tydelige?	○	○	○	○	○



NTNU
Kunnskap for en bedre verden

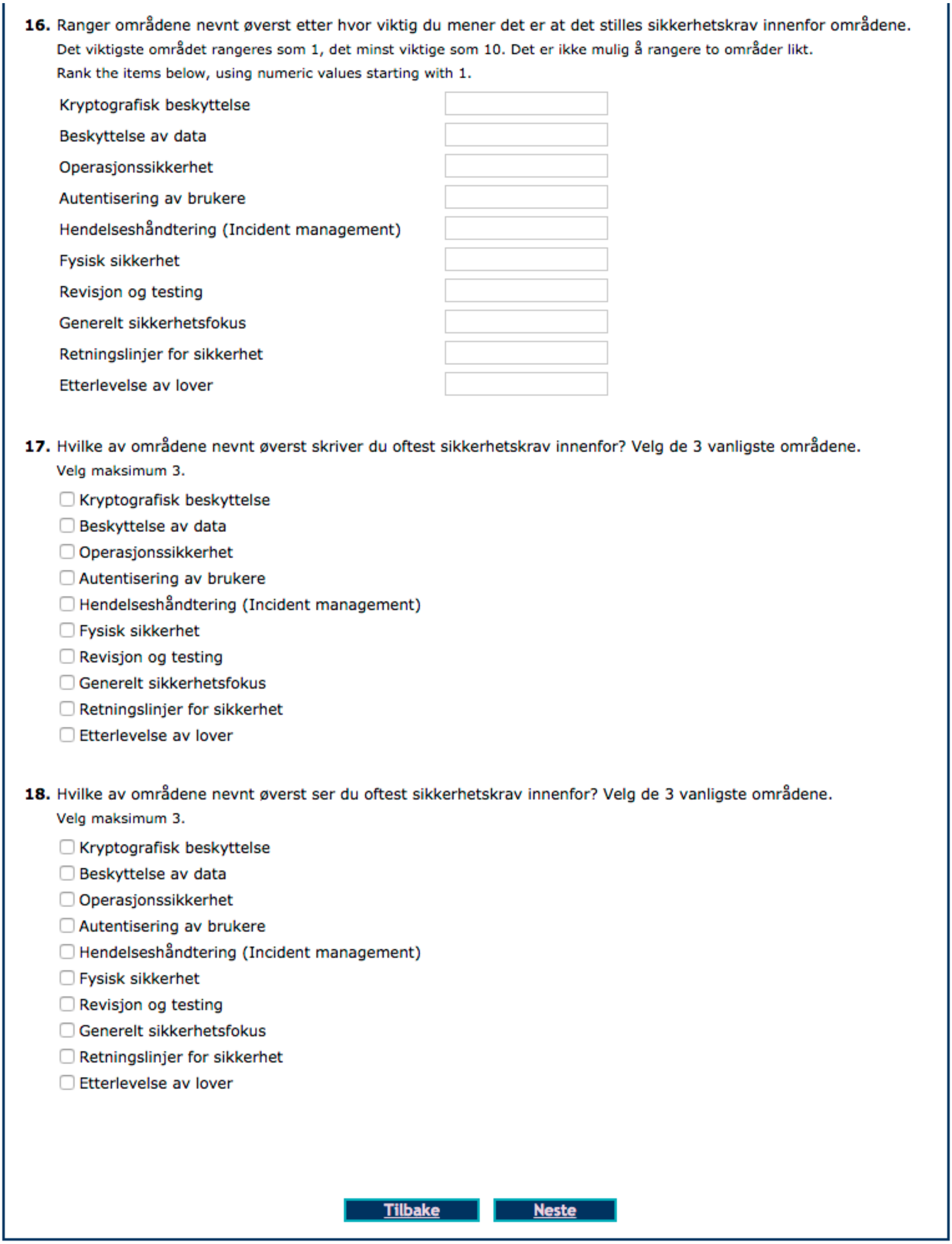
Security Requirements in Public Procurement

Side 6 av 7

Områder for sikkerhetskrav

På denne siden vil du få spørsmål om områder det kan stilles sikkerhetskrav innenfor. For å hjelpe deg forstå innholdet i de ulike områdene gis det her noen eksempler:

Område	**Eksempler**
Kryptografisk beskyttelse	Kryptering av data på åpne nett Nøkkelhåndtering (Key management) Operasjonsmodus (Mode of operation)
Beskyttelse av data	Håndtering av data Transport av data
Operasjonssikkerhet	Beskyttelse fra skadevare og virus Backup Logging
Autentisering av brukere	Brukerautentisering Brukeridentifisering Tilbakekalling og utløp av brukerrettigheter
Hendelseshåndtering (Incident management)	Detektering av datainnbrudd Rapportering av sikkerhetshendelser
Fysisk sikkerhet	Detektering av fysiske angrep Sikre områder
Revisjon og testing	Sikkerhetsrevisjon Ekstern testing Revisjonslogging
Generelt sikkerhetsfokus	Holde systemer oppdaterte Endringskontroll
Retningslinjer for sikkerhet	Informasjonssikkerhetspolicy
Etterlevelse av lover	Etterlevelse av lover og forskrifter



16. Ranger områdene nevnt øverst etter hvor viktig du mener det er at det stilles sikkerhetskrav innenfor områdene.

Det viktigste området rangeres som 1, det minst viktige som 10. Det er ikke mulig å rangere to områder likt.

Rank the items below, using numeric values starting with 1.

Kryptografisk beskyttelse	
Beskyttelse av data	
Operasjonssikkerhet	
Autentisering av brukere	
Hendelseshåndtering (Incident management)	
Fysisk sikkerhet	
Revisjon og testing	
Generelt sikkerhetsfokus	
Retningslinjer for sikkerhet	
Etterlevelse av lover	

17. Hvilke av områdene nevnt øverst skriver du oftest sikkerhetskrav innenfor? Velg de 3 vanligste områdene.

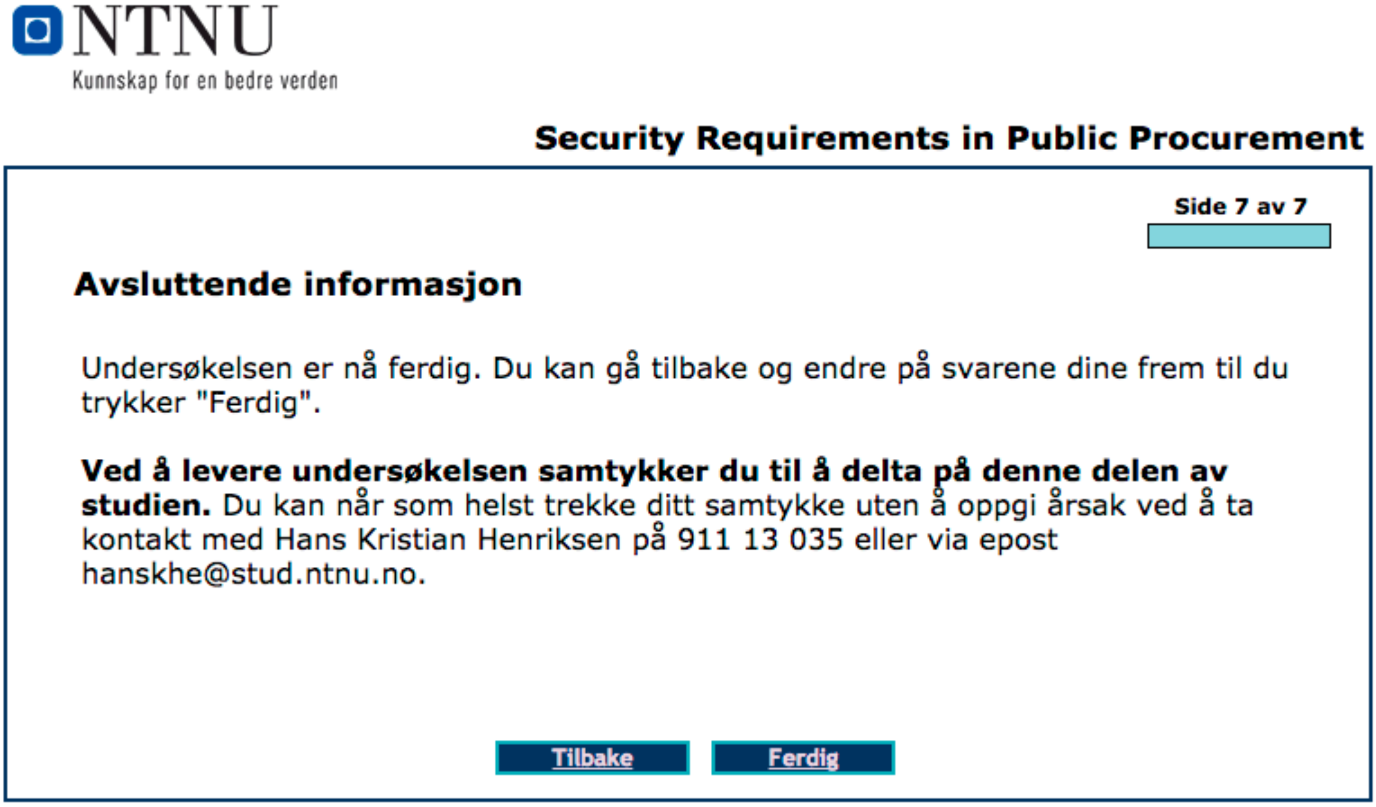
Velg maksimum 3.

□ Kryptografisk beskyttelse
□ Beskyttelse av data
□ Operasjonssikkerhet
□ Autentisering av brukere
□ Hendelseshåndtering (Incident management)
□ Fysisk sikkerhet
□ Revisjon og testing
□ Generelt sikkerhetsfokus
□ Retningslinjer for sikkerhet
□ Etterlevelse av lover

18. Hvilke av områdene nevnt øverst ser du oftest sikkerhetskrav innenfor? Velg de 3 vanligste områdene.

Velg maksimum 3.

□ Kryptografisk beskyttelse
□ Beskyttelse av data
□ Operasjonssikkerhet
□ Autentisering av brukere
□ Hendelseshåndtering (Incident management)
□ Fysisk sikkerhet
□ Revisjon og testing
□ Generelt sikkerhetsfokus
□ Retningslinjer for sikkerhet
□ Etterlevelse av lover



Security Requirements in Public Procurement

Side 7 av 7

Avsluttende informasjon

Undersøkelsen er nå ferdig. Du kan gå tilbake og endre på svarene dine frem til du trykker "Ferdig".

Ved å levere undersøkelsen samtykker du til å delta på denne delen av studien. Du kan når som helst trekke ditt samtykke uten å oppgi årsak ved å ta kontakt med Hans Kristian Henriksen på 911 13 035 eller via epost hanskhe@stud.ntnu.no.

Appendix B

Interview guide

This appendix presents the interview guide used during the interviews. The guide is in its original Norwegian. At the top of each page are the fields used to note the participant's unique identifier as well as which categories of questions should be asked the participant.

Identifikator:	Spørsmål:

#	Spørsmål	Presisering, utbrodering (Dypere)	Oppfølging (Bredere)
	Oppvarming		
1 F	Kan fortelle meg litt om arbeidshverdagen din?	• Hvilke arbeidsoppgaver har du? • Arbeider du mye i team?	• Hva går tiden med til? • Hva er mest spennende?
	Generelt om anbudsprosessen		
2 F	Hvor sentralt mener du det er at sikkerhetskrav er ferdig utformet når et anbud sendes ut til tilbyderne?	• Et moteksempel ville f.eks. vært at sikkerhetskrav ikke er definert, men del av betingelsene i en rammeavtale. eller • Brede krav: "Kunden skal sørge for god sikkerhet i løsningen" • Hvorfor? • Hva er konsekvensen av at dette ikke gjøres?	• Hva mener du er den beste måten å løse dette på? •
3 F	*Fra undersøkelsens spm 7:* ***L:****(Hvis du skal sette deg i skoene til de som skriver anbud)* Hvordan mener du anskaffelsesprosessen påvirker muligheten til å stille gode sikkerhetskrav?	• Det er en del begrensninger i anskaffelsesprosessen, f.eks. knyttet til endringer, kommunikasjon med tilbydere, osv. Påvirker noen av disse muligheten til å stille gode krav? • Er det noen hindre? • Er det noe som tilrettelegger for gode krav?	• Hva er den viktigste endringen man kunne gjort i anskaffelsesregelverket for å gjøre det enklere å arbeide med sikkerhetskrav?

Identifikator:	Spørsmål:

#	Spørsmål	Presisering, utbrodering (Dypere)	Oppfølging (Bredere)
4 F	*Fra undersøkelsens spm 7:* **A:***(Hvis du skal sette deg i skoene til de som besvarer anbud)* Hvordan mener du anskaffelsesprosessen påvirker muligheten til å oppfylle sikkerhetskrav på en god måte?	• Det er en del begrensninger i anskaffelsesprosessen, f.eks. knyttet til endringer, kommunikasjon med tilbydere, osv. Påvirker noen av disse muligheten til å oppfylle krav på en god måte? • Er det noen hindre? • Er det noe som tilrettelegger for besvarelse?	• Hva er den viktigste endringen man kunne gjort i anskaffelsesregelverket for å gjøre det enklere å arbeide med sikkerhetskrav?
5 A	Hva mener du er viktigst for en anbudsgiver å kommunisere med sine sikkerhetskrav?	• Er det konkrete funksjoner, eller f.eks. sikkerhetsmål? • Hvorfor? • Hva er det som gjør det viktig?	• Er det noe man bør unngå å kommunisere?
6 L	Hva mener du er viktigst for deg som leverandør at kommuniseres i sikkerhetskrav?	• Er det konkrete funksjoner, eller f.eks. sikkerhetsmål? • Hvorfor? • Hva er det som gjør det viktig?	• Er det noe man bør unngå å kommunisere?
	Konkret i bedriften		
7 A	Hvordan går du/dere frem for å skrive sikkerhetskrav?	• Kan du beskrive prosessen mer detaljert? • Hva tar dere utgangspunkt i når dere skal lage sikkerhetskrav? • Gjenbruker dere sikkerhetskrav fra tidligere prosjekter?	• Hva er bakgrunnen for at dere bruker denne prosessen?

Identifikator: Spørsmål:

#	Spørsmål	Presisering, utbrodering (Dypere)	Oppfølging (Bredere)
8 A	Hvor sentralt er sikkerhetskrav når kravspesifikasjonen skal skrives?	• Når i prosessen utformes sikkerhetskravene?	• <Se opp mot svaret på #2>
9 A	Opplever dere at dere kun får den sikkerheten dere ber om?	• Leveres det noen ganger systemer med mer sikkerhet enn det man har bedt om i anbudet?	
10 A	Har du noen eksempler på tilbakemelding fra leverandører på sikkerhetskrav du har utformet?	• Enten i forbindelse med anbudsprosessen, eller under implementering?	• Er det vanlig/mulig å få tilbakemeldinger fra leverandører på krav som stilles?
11 L	Hvordan går du/dere frem når sikkerhetskrav skal besvares/oppfylles?	• Kan du beskrive prosessen mer detaljert? •	
12 L	Implementerer dere kun den sikkerhet kunden ber om?	• Vurderer dere det noen gang slik at sikkerhetskravene er for dårlige, og implementerer mer enn det som forespørres?	• Hvordan påvirker brede/ vage sikkerhetskrav den sikkerhet som leveres?
13 L	Hvordan opplever du de sikkerhetskrav du bidrar til å besvare?	• Kan du si noe generelt om kvaliteten? • Hvor enkle er kravene å forstå?	
14 L	Har du noe eksempel på tilbakemeldinger du har gitt til anbudsgiver på sikkerhetskrav	• Enten i forbindelse med anbudsprosessen, eller under implementering?	• Er det vanlig/mulig å gi tilbakemeldinger til anbudsgiver på krav som stilles?

Identifikator:	Spørsmål:

#	Spørsmål	Presisering, utbrodering (Dypere)	Oppfølging (Bredere)
15 F	Hvor stor mulighet for kommunikasjon og tilbakemelding på sikkerhetskrav er det mellom anbudsgiver og leverandør?		- Brukes denne muligheten? - Kunne du tenkt deg mer kommunikasjon mellom anbudsgiver og leverandør?
	Konkrete krav I undersøkelsen ble du bedt om å vurdere en rekke sikkerhetskrav. Jeg vil gjerne at vi skal se nærmere på noen av dem.		
16 F	Hva tenker du om dette sikkerhetskravet?	Du har svart at… Kan du utdype hvorfor du mener det? Sammenlignet med en del andre… Hva tenker du om denne forskjellen?	- Hvordan ville du har formulert et tilsvarende krav?
	Avsluttende generelle spørsmål		
17 F	Mener du at sikkerhetskrav har blitt viktigere de siste årene?	- Hvorfor? - Er det noen enkeltområder som har blitt viktigere?	
18 F	Hva mener du er et godt sikkerhetskrav?	- Hvilke egenskaper har et godt sikkerhetskrav? - Hva må man unngå i et godt sikkerhetskrav?	

Identifikator: Spørsmål:

#	Spørsmål	Presisering, utbrodering (Dypere)	Oppfølging (Bredere)
19 F	Er det sikkerhetskravene som avgjør om vi får god sikkerhet i løsningene våre, eller er det andre faktorer?	• **Nei:** Burde vi da fokusere så mye på sikkerhetskrav? • Hva bør vi i stedet fokusere på? • **Ja:** Fokuserer vi da nok på sikkerhetskrav? • Hvordan kan vi sørge for at sikkerhetskrav står sentralt i anbudsprosessen?	
20 F	Hva kan man gjøre for å enkle arbeidet med sikkerhetskrav i offentlige anskaffelser?	• Kan utarbeidelse av gode veiledere, enkle anbefalinger eller eksempelkrav hjelpe?	
	Avslutning		
	Har du noe mer du vil snakke om, som du ikke føler du har fått mulighet til så langt?		
	Har du noen spørsmål, enten til undersøkelsen, databehandling eller noe annet?		

Appendix C

Consent form

This appendix includes the consent form sent to the participants. The form was modelled on the example consent form issued by the Norwegian Social Science Data Services to ensure all necessary information was included. It is presented only in the original Norwegian version sent to the participants.

Forespørsel om deltakelse i forskningsprosjektet

”Security requirements in Norwegian Public Procurement”

Bakgrunn og formål
Studien gjennomføres på bakgrunn av en forstudie gjennomført høsten 2015 hvor det ble funnet svært varierende sikkerhetskrav i et utvalg på 29 offentlige anskaffelser. Denne studien har som formål å undersøke hvordan sikkerhetskrav stilles, og hvilke vurderinger som gjøres i denne prosessen hos de offentlige etater som publiserer anbudsdokumenter. I tillegg vil studien undersøke hvordan sikkerhetskravene oppfattes, tolkes og implementeres av de firmaer som oppfyller anbud.

Studien gjennomføres som en masteroppgave ved Institutt for Datateknikk og Informasjonsvitenskap ved Norges teknisk-naturvitenskapelige universitet (NTNU).

Utvalget i studien er rekruttert fra studentens og veileders nettverk.

Hva innebærer deltakelse i studien?
Studien gjennomføres ved at deltakerne først får tilsendt en spørreundersøkelse. Denne inneholder en seksjon med generelle spørsmål slik at intervjuer kan forberede seg til intervjuet. I tillegg er det spørsmål vedrørende sikkerhetskrav, hvordan disse stilles/oppfylles og hva som oppfattes som et godt sikkerhetskrav. Spørreundersøkelsen tar ca 15 minutter å besvare.

Etter at spørreundersøkelsen er besvart gjennomføres et intervju med deltakeren. Intervjuet er ment til å gi deltakeren mulighet til å utdype svarene i spørreskjemaet, samt å skape rom for en samtale rundt teamet. Intervjuet vil følge en semi-strukturert fremgangsmåte, hvor det er rom for å avvike fra de forhåndsbestemte spørsmålene for å utforske tema som kommer opp under intervjuet. Intervjuet vil bli tatt opp på bånd for å forenkle transkripsjonen, og for å korte ned gjennomføringstiden. Intervjuet vil ta ca 30-45 minutter.

Hva skjer med informasjonen om deg?
Alle personopplysninger vil bli behandlet konfidensielt. Opplysningene er kun tilgjengelig for studenten som gjennomfører studien, samt veileder og biveileder ved hhv. Institutt for Datateknikk og informasjonsvitenskap (NTNU) og Institutt for telematikk (NTNU). Alt materiale fra undersøkelse og intervju (inkludert lydopptak) vil bli lagret på låst kontor i låst skap på universitetet. Koblingsnøkkel oppbevares separat fra resten av materialet. Data fra spørreundersøkelsen lagres på NTNUs egne servere, og sendes ikke ut av landet.

Deltakerne vil ikke kunne gjenkjennes i det publiserte materialet. Alle opplysninger vil bli anonymisert, og deltakers navn, stilling, arbeidsplass og annen identifiserende informasjon vil ikke bli publisert.

Prosjektet skal etter planen avsluttes 01.07.2016. Ved avslutning av prosjektet vil alle data anonymiseres. Lydopptak av intervjuer vil bli slettet, og transkripsjoner og notater anonymisert. Koblingsnøkkel for datamaterialet vil bli destruert.

Frivillig deltakelse
Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi noen grunn. Dersom du trekker deg, vil alle opplysninger om deg bli anonymisert.

Dersom du har spørsmål til studien, ta kontakt med Hans Kristian Henriksen på telefon 911 13 035. Hovedveileder og daglig ansvarlig for datainnsamlingen er John Krogstie, og kan kontaktes på telefon 934 17 551.

Studien er meldt til Personvernombudet for forskning, Norsk samfunnsvitenskapelig datatjeneste AS.

Samtykke til deltakelse i studien

Jeg har mottatt informasjon om studien, og er villig til å delta

----
(Signert av prosjektdeltaker, dato)

Signert skjema kan scannes og sendes til hanskhe@stud.ntnu.no, eller returneres pr post til

Institutt for Datateknikk og Informasjonsvitenskap NTNU
att: Hans Kristian Henriksen
7491 Trondheim

Appendix D

Introductory information

This appendix presents the notes for the introductory information given to the participants of the study before conducting the interviews. The notes were used as guidelines, and not read to the participants word by word.

Innledende informasjon

Aller først vil jeg gjerne takke deg for at du har tatt deg tid til å delta i denne studien. Målet mitt er at resultatene skal kunne bidra til å gi anbefalinger om hvordan sikkerhetskrav bør utformes i offentlige anbud. I tillegg håper jeg å øke kunnskapen om hvordan de ulike sidene av anbudsprosessen oppfatter sikkerhetskrav.

Før vi begynner, så vil jeg gå igjennom de personvernhensyn som tas med tanke på de data vi samler inn. Alle opplysninger behandles konfidensielt, og er kun tilgjengelig for meg, og evt. mine veiledere. Alle data er anonymisert, og det finnes en koblingsnøkkel som knytter svarene til personer. Denne oppbevares innelåst, og destrueres når studien avsluttes. For å korte ned intervjutiden, og for å gjøre det mulig for meg å gå igjennom intervjuet i etterkant, tas det opp på bånd. Det er kun jeg som har tilgang til opptakene, og de slettes så snart de er transkribert.

Det vil ikke fremgå navn, stilling eller bedriftsbeskrivelse i det publiserte materialet. Det eneste som vil bli knyttet til sitater og tall er om det kommer fra en anbudsgiver eller en tilbyder.

Du har fått tilsendt et samtykkeskjema, som også inneholder informasjon om undersøkelsen. Du kan når som helst trekke ditt samtykke til å delta uten å oppgi noen grunn. Du kan også i løpet av intervjuet si at det er enkelte spørsmål du ikke vil svare på.

Har du noen spørsmål før vi begynner?