Norges teknisk-
naturvitenskapelige
universitet

TDT4501 - Computer Science, Specialization Project

Security Requirements in Norwegian Public Procurement

Hans Kristian Henriksen

Fall 2015

PROJECT THESIS

Department of Computer and Information Science

Norwegian University of Science and Technology

Supervisor: Professor John Krogstie, IDI

External Supervisor: Lillian Røstad, Difi

Preface

This report is the final deliverable of my project thesis at the Norwegian University of Science and Tehcnology. It was written in the autumn of 2015 as part of the 9th semester of my master studies in computer science.

The project was proposed by Lillian Røstad at Difi, who has also been my external advisor.

Readers of the report are assumed to be somewhat familiar with the topic of information security.

Trondheim, 16/12-2015

(Signature)

Hans Kristian Henriksen

Acknowledgment

Working on a report of this size, and a source material as extensive, has been a real challenge. Many cups of coffee and tea has 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 report.

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 report that I am very proud of.

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

Professor Guttorm Sindre at IDI helped me get started by providing relevant research at the very beginning of the project.

Working through both day and night for many months has been hard on both my girlfriend and family, whom I have not spent as much time with as I should. For their support and understanding, I am ever grateful.

H.K.H.

Abstract

With IT-systems becoming an omnipresent part of life, storing and processing almost all our information, it is imperative that these systems be secure against both malicious attacks and unintended failures that can lead to the disclosure, altering or destruction of vital information. This report looks into the security requirements given in Norwegian tenders for IT-systems and services.

In this report, three research questions are put forward: 1. Which information security requirements are set by the government when acquiring IT-systems? 2. What does the theory say - what recommendations for defining requirements when acquiring IT-systems exists? 3. What is the gap between recommendations and reality - is there a large deviation, or a large correspondence?

Seven main recommendations are identified in the literature. Additionally, Common Criteria, ISO 27002, and PCI-DSS are reviewed, and the common factors of these standards are identified. This is used to analyse the security requirements of 29 tenders for IT-systems and -services.

The findings show that the state of security requirements in Norwegian public procurements is varied and not in line with most of the recommendations. No correlation between security requirements in line with the recommendations and system size or cost is found, nor with organisation type or size. The *number* of security requirements appears to be positively correlated with the number of system requirements, though a high number of security requirements is not necessarily correlated with high quality security requirements.

Most troubling is that 18 of the studied 29 tenders have no requirements for the use of security standards, and that 7 tenders presented either one or zero security requirements.

Further work in the field should focus on the elicitation process for security requirements, and how security requirements are interpreted and implemented by the suppliers. Similar research should also be done in both EU and non-EU settings. Improvements in automatic requirements analysis could help the purchasers define better requirements.

Contents

Preface i

Acknowledgment ii

Summary and Conclusions iii

1 Introduction **1**

1.1 Background 1

1.2 Research questions 2

1.3 Limitations 3

1.4 Approach 3

1.5 Structure of the Report 3

2 Method **4**

2.1 Procurement documents 4

2.2 Theory 6

2.3 Alternative methods 6

2.4 Ethics 7

3 Procurement process **8**

3.1 Goal of procurement 8

3.2 Regulation 9

3.3 Competition types 9

3.4 The procurement process 10

3.5 Challenges in public procurement 12

4 State of the art 13
4.1 Discussion of sources 13
4.2 Defining security requirements 14
4.3 Recommendations in the literature 15
4.4 Standards 19
4.5 Data processor agreement 30

5 State of the practice 31
5.1 Overview of selected tenders 32
5.2 Security requirements in selected tenders 33
5.3 Recommendations from the literature 36
5.4 Documents without security requirements 46
5.5 Data processor agreements 47

6 Conclusion 48
6.1 Literature recommendations 48
6.2 Requirements in studied tenders 49
6.3 Possible weaknesses 52
6.4 Application outside Norway 53
6.5 Further work 53

Bibliography 60

A Overview of studied tenders 61

B Translated requirements 62
B.1 Gather security requirements in one place 62
B.2 Security requirements should not place unnecessary constraints on the system . . 63
B.3 Security requirements should not be too open or vague 63
B.4 Well known standards should be followed 64

Chapter 1

Introduction

This chapter will present the background for the problem at the core of this report, a precise problem formulation with specific research questions, and a motivation to why these are interesting and important questions to answer.

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 [1]. As part of this, 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] [2]

When a tender is published, the purchaser can no longer make changes to the process, or significant changes to the documents that has been published. The consequence of this is that 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, non of which are further discussed in this report.

[2] This is obviously a simplification of the more than 25 000 word regulation that govern this area, but it is sufficient to give an introduction to the procurement process. The process is further discussed in chapter 3.

Problem Formulation

The report is based on a problem set forth by Lillian Røstad, at Difi:

> As 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.

Motivation

The motivation for pursuing an answer to the given problem is to be able to evaluate the security requirements in tenders put forth by the Norwegian government. According to numbers from 2012, the Norwegian government uses approximately 20 billion NOK [3] every year in procurement of IT-systems and services. With this large amount 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 being able to understand what requirements are set for security, and to contribute to the improvement of security requirements given. The ultimate goal of this report is 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.

1.2 Research questions

For this project, the following research questions have been identified:

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?

1.3 Limitations

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 is obviously impossible to go trough all documents. As described in chapter 2, a selection of documents was chosen for review.

1.4 Approach

To be able to answer the research questions defined, there was a need for a large amount of literature on the subject. This has been gathered through the help of Prof. Guttorm Sindre at NTNU, as well as trough internet searches, using Google Scholar, Science Direct, IEEExplorer and NTNU University Library BibSys.

Information on the tenders put out by the government has been collected using Doffin, the database for public procurement, as well as direct contact with purchasers.

1.5 Structure of the Report

In chapter 2, the method used in the work with this report is presented. In chapter 3, an introduction to the procurement process is given. Chapter 4 presents the current state of the art on the subject. This is followed by a presentation of the security requirements that are given in the studied tenders in chapter 5. In chapter 6 the conclusions of the findings are presented, and fields of further work are given. Appendix A gives an overview of the selected tenders. Appendix B gives the original Norwegian wording of all translated tenders.

Chapter 2

Method

This report sets out to answer the research questions given in section 1.2. From this, it is clear that a literature study needs to be conducted in order to answer RQ2 and RQ3. RQ1 pertains to the requirements given in requests for tenders. It will therefore be necessary to acquire a selection of procurement documents, and analyse their contents. In this chapter the methods used to answer the research questions will be outlined, and a rationale to this choice provided.

2.1 Procurement documents

The calls for tenders of all publicly available procurements are published in Doffin, the database for public procurement.[1] All information in the database is publicly accessible and searchable. While this will provide a lot of information on the tenders, specification documents are not always included in the published part of the tender. In these instances, the responsible government agency was contacted with a request for access 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) [4].

Out of 27 requested documents, 2 where not released in any form, based on section 23 paragraph 3 of the freedom of information act, which states that documents pertaining to a public procurement may be withheld until the selection of a supplier has been made. In addition to

[1] 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.

these documents, Lillian Røstad put out a call for tender documents to her network, providing an additional four tenders. This leaves 29 tenders to be studied in this report.

2.1.1 Selection and organisation

As stated in the introduction, more than 500 tenders have been published in the IT-sector alone within the 12 months preceding the work on this project. Going through all documents for each one would have been an enormous task. To be able to quickly select interesting tenders that documents should be requested for, it was decided to select tenders that:

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

This is obviously not a method that will yield completely objective results. Systems that seemed interesting to the author may have been disproportionally selected. Making sure that no organizations were overrepresented, as well as selecting a significant number of tenders are measures taken to ensure that the selection was as representative as possible.

2.1.2 Non-disclosure

Some of the documents that were acquired during this project were released under the condition that specifics were not to be presented in this report without consulting the document owner. There are different reasons for the conditions set by the document owners. Some of the documents in question were exempted from public access, either because the competition was not yet completed, or for other reasons in accordance with the Freedom of information act (Offentleglova). In a couple of cases the documents were eligible for release under the Freedom of information act, but the document owner still requested to be kept informed of the use of specific quotes. While this is not required by law, the author has chosen to respect the wishes of these owners, as long as it does not threaten the integrity of the report.

Where examples from any of these documents were relevant to this project, the document owner was contacted and asked for permission to publish specific requirements. No requests for use of quotes from documents were declined.

2.2 Theory

My advisor at Difi, Lillian Røstad was not aware of any research into the field of *security* requirements in public procurement, and initial searches for theory did not return documents on the subject. As a consequence of this, a more thorough literature search had to be conducted.

2.2.1 Literature searches

Gaining an overview and understanding of the research in the area was the first task to be conducted. To make a systematic effort, a set of search queries were defined, and run trough the largest and most relevant databases of scientific research. Google Scholar, Science Direct, and IEEE Xplore were searched with the following queries:

- computer (procurement OR tender)
- requirements (procurement OR tender)
- requirements engineering acquisition

In addition to searching for documents that deal with requirements in the context of procurement processes, background material on both the subjects of requirements and the subject of procurements and tenders was needed. Searches for literature in these fields were done trough the same databases, and an assortment of articles chosen based on their abstracts. The result of the literature review is given in chapter 4.

2.3 Alternative methods

There are alternatives to the methods chosen in this report. To answer the question of what requirements are set by the government when acquiring IT-systems, a series of interviews with product owners and suppliers could have been conducted. This would in addition have made it possible to ask questions about why certain choices were made, as opposed to just analysing them theoretically. Answering the research questions in this project however, calls for a method that analyses a large set of tenders, and doing this in interview form would be a daunting task. In addition to this, the vendors have to respond to the requirements in the call for tender, not the requirements that exists in the heads of the people who wrote the requirement. This made it natural to analyse the requirements in the same way a vendor would.

In future work on the subject, interviews can be interesting in determining the reasoning behind some of the requirements, and to understand the process behind producing tender documents. This would call for a deeper dive into specific requirements and purchases. More on future work can be found in section 6.5.

2.4 Ethics

In all research there are ethical aspects to consider. The work with this report has not involved the use of experiments on people, the collection of personal information, or other research activities that would normally require rigorous ethical planning.

The main ethical concern in the work with this report has been the use of some of the tender documents that were acquired. While most of the documents were released under the Freedom of information act (Offentleglova), some were not ready for release at time this report was written, as described in section 2.1.2. Maintaining the confidentiality of these documents has been central in the work on this report. All use of the documents have been cleared with the document owners.

The owners of some of the documents that were public information wanted to be informed of any use of the documents. While this is not required by law, all such requests were honoured. The cooperation of the document owners has been vital for this report, and it only seemed fitting to respect their wishes of being kept up to speed, as long as this was not at the expense of the scientific integrity of the research.

Chapter 3

Procurement process

The procurement process is a complex legal field which could be the subject of several master theses of law. It is not the goal, nor in the scope of this report, 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.

3.1 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 varies with the situation of the country that is studied, but for most countries the central goals are to get products that have high quality, at low cost, delivered in short time. Procurement also raises the competition level in the market, can be used to encourage innovation, meet environmental and social goals, and is meant to ensure fair competition amongst different suppliers. [5,6] 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"*. [7]

3.2 Regulation

Public procurement is regulated through Law on public procurement [7], and Regulation on public procurement [2]. As part of the European Economic Area, Norway is bound by the european laws in this field. This has 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. [8]

3.3 Competition types

When publishing a tender, there are four types of competition that can be used. Depending on the tender, not all may be allowed, and some will be more fitting than others. Below follows a short description of each competition type.

3.3.1 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 this 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 requirements. [9]

3.3.2 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 expect 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. [9]

3.3.3 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, as in restricted competition. The negotiations 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. [10]

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 the cancelation of the tender. [10]

3.3.4 Competitive dialogue

Competative dialogue is only allowed if the contract 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 [11]. 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 dialog 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. [12, 13]

3.4 The procurement process

Procuring a product or service is a long process, that involves several steps. A short overview of the process is given in figure 3.1. Based on [14] 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 need of the organisation is 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 3.3 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 this is announced. Given that there are no complaints (in 2014, The Norwegian Complaints Board for Public Procurement (KOFA) processed 276 complaints regarding procurement processes [15]) the contract can be signed, and delivery start. The last phase is to ensure that the correct product is delivered, make payment, and conclude the contract.

This report is focused on the documents that are published in phase 4 of figure 3.1. The process behind eliciting and defining the requirements (phase 3), how requirements are interpreted by the suppliers (phase 4 and 5), and whether the final product (phase 6) fulfils the needs and purpose of the organisation (phase 1 and 2), is outside the scope of this report. This is however suggested as areas of future work, see section 6.5.

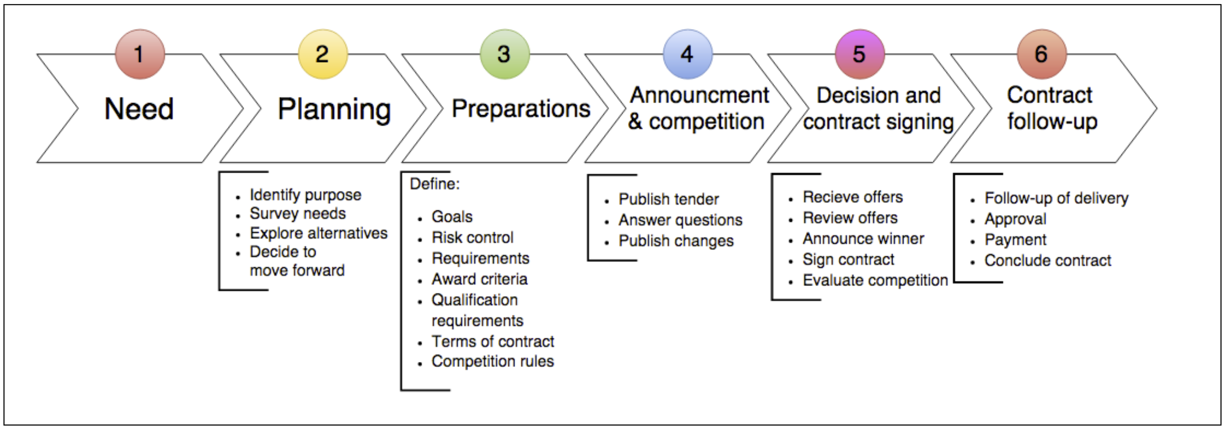

Figure 3.1: Simplified view of the tender process, based on [14]

3.5 Challenges in public procurement

One of the central factors separating the tender 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 [16]. Because of this, all requirements must be well considered before the tender is put forth [17]. 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 [2].

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 to this, the questions and their answers are made available to all other suppliers to ensure a fair process. This is a deterrent to asking questions, as it might reveal parts of the offer a supplier wants to submit. [18]

Chapter 4

State of the art

In this chapter, the current state of the theory on the subject of security requirements is put forth. Section 4.1 gives a quick discussion of the sources used. In section 4.2 the definition of security requirements used when evaluating the tenders is given. Section 4.3 presents the recommendations from the literature, and section 4.4 provides a look at three current security standards, and what they have in common. Lastly, section 4.5 briefly discusses data processor agreements.

4.1 Discussion of sources

There is a lot of literature on the subject of security requirements. This makes the process of selecting relevant articles and other source material challenging. Professor Guttorm Sindre at the Department of Computer and Information Science at NTNU helped in the selection of some background documents.

However, a lack of information on the subject of security requirements in the context of tender processes became apparent early in the research phase. Little literature was found that related directly to the main questions of this report. Prof. S. Lauesen at the University of Copenhagen seems to be one of the only people who have done any substantial research into the field. This is corroborated by Paech et. al. [18]:

> "Very few papers have been published dealing with [requirements engineering] for tender processes. Lauesen is one of the few exceptions."

Lauesens research is then, naturaly, of great interest. It does not touch on the specific topic of *security* requirements, but general challenges in requirements engineering is most likely also an issue for security related requirements. Other than this, finding relevant research has proven difficult. This has lead to an approach where the procurement process, as well as security requirements are studied. Based on this, the goal is to be able to say something about good security requirements, and how the procurement process affects the ability of purchasers to follow guidelines for security requirements.

4.2 Defining security requirements

Before we can look at the literature on the subject of requirements, and more specifically security requirements, it is useful to gain an understanding of different definitions of security requirements. [19] defines security requirements as

> "constraints on the system's functional requirements (...)"

while Firesmith has the following definition:

> "A security requirement is typically a detailed requirement that implements an overriding security policy." [20]

Tondel et. al [21] in their survey of techniques for eliciting security requirements writes:

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

This highlights the first of many challenges in this field. If experts on the subject can not agree on a definition of a security requirement, how can we expect anyone to be able to formulate a good requirement?

For the analysis of the tender documents described in chapter 5, we need a working definition of security requirements. Many suppliers have used their own definition to assign requirements into the category *security*. These requirements have been regarded as security requirements[1], as that is how they are presented to the suppliers. In addition, requirements that

[1] In some tenders, the section for security requirements has been mixed with other categories clearly not pertaining to security. In these cases, the requirements that did not fit into any of the categories in section 4.4.4 have been ignored.

describe a security policy, constrains the system's functionality for security or privacy reasons, and any requirement that fits into one of the categories identified in 4.4.4, has been regarded as a security requirement.

To make the analysis of the security requirements simpler, complex requirements, or requirements that encompass more than one of the categories in section 4.4.4, have been broken down into several requirements.

4.3 Recommendations in the literature

With this foundation, it is time to look into the recommendations that can be found in the literature. As mentioned in section 4.1, it has proven difficult to find literature that specifically pertains to the question of security requirements *in public procurement*. This section will summarise the recommendations on security requirements that were found, and attempt to put them in the context of public tenders.

4.3.1 Gather security requirements in one place

> "We suggest describing all security requirements in one place, preferably as part of a general requirements document, to retain an overview of all requirements." [21]

Starting of easy, Tøndel et. al. suggests gathering all security requirements in a single place. This is an argument that is not difficult to understand. Tenders can easily have several hundred requirements spread over several documents. Having to go through multiple documents to find the security requirements would increase the risk of missing some of them. Security requirements that are placed in other sections of the document may also become inconsistent with the rest, as they may not be updated with the others [22]. Given the size of some tenders, this can become a real issue.

Some tenders have several contracts connected to the tender, e.g. one for development and one for operations. In these cases, there might be legal reasons for having to spread security requirements over multiple documents. This is probably the most likely way for the tender process to hinder gathering of security requirements.

4.3.2 Security requirements should not place unnecessary constraints on the system

> "Thus, the most common problem with security requirements, when they are specified at all, is that they tend to be accidentally replaced with security-specific architectural constraints that may unnecessarily constrain the security team from using the most appropriate security mechanisms for meeting the true underlying security requirements." [20]

The challenge presented here by Firesmith is requirements that become a barrier to develop the most secure system possible. A requirement may specify a certain security technology or protocol, which could become obsolete at the time of development. The supplier may then be prevented from choosing the most up to date technology, even though this would benefit the customer.

If for example an encryption technology used for transfer over HTTPS is specified, this might stop the supplier from choosing to transfer data over another protocol, even if this would make the solution both safer and more efficient. As the procurement process generally does not allow the purchaser to alter the requirements of the tender after it is issued, an inferior solution might have to be chosen.

4.3.3 Security requirements should not be too open or vague

> "For some of the open requirements (...), none of the suppliers had a solution." [23]

On the other side of requirement complexity, we have the requirements that are too open. This can become a problem both at the competition stage, and when the system is to be implemented. Requirements that are too open become difficult for the supplier to answer. There is usually little time to answer a tender, and for an open requirement it can be complicated to propose a solution in a short time frame. It can also be difficult to understand what the customer really wants to have delivered when the requirements are vague. There is some room to ask the purchaser clarifying questions, but these questions, along with the answers, are made available to all competitors for the same tender. The supplier then runs the risk of indirectly disclosing parts of their bid, or business secrets, to their competitors. [18]

For the purchaser, presenting requirements that are too open puts them at risk of taking delivery of a system that does not perform as envisioned. The customer may have had an idea of what the solution would be, while the supplier has interpreted the requirements differently. [24] As long as the requirements can objectively be determined as fulfilled, the system would have to be accepted.

One way of writing vague requirements is using qualitative statements that are difficult to quantify, and thus impossible to objectively verify. In their work to make an automatic tool to analyse requirements, Lami et. al. [22] presents a set of characteristics for requirements. They describe requirements as vague if they contain words such as *clear, easy, strong, good, bad.* Requirements containing this type of words are difficult to fulfil and evaluate, and should therefore be avoided, especially for security related requirements.

4.3.4 There should be a consistent selection of security requirements

> "In several of the specifications studied we note that some relevant security areas are fairly well specified whereas other are completely left out." [25]

It is important to see the relationships between different security requirements. There is no reason to lock valuables inside a safe, if the safe is light and not attached to the floor. The same is true for information security; securing an application is no good if the server room is easy to break into. In terms of writing security requirements, this means that one must consider how one requirement might entail a number of other requirements.

To exemplify this, Wilander and Gustavsson describes requirement documents where there are good requirements regarding access control and roles, but no requirements for encryption or physical security. This describes a scenario where it appears important for the customer that access to the information is restricted, but where the customer fails to take into account other attack vectors that would also lead to disclosure of the information. [25]

Again, because of the inflexible nature of the tender process, these concerns must be addressed during the requirement elicitation phase.

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

> "Some security requirements have a high level of detail whereas others in the same specification are only specified on a general level." [25]

Given a requirement specification that varies in detail, the supplier may get the impression that some of the areas are more important than others. This can also give the impression that the other parts of the specification are not an area of focus for the purchaser, and thus not something to spend too much time on when writing an offer. If user authentication is specified using a number of requirements, while incident management is given none, or few requirements, it is to be expected that the supplier will regard incident management as far less important.

This kind of inconsistency can arise from what Willander and Gustavson [25] call *local heroes*. This is a person with substantial knowledge on some fields, and who makes sure that these fields are covered in detail in the requirements specification. Areas that does not have their own local hero are often neglected, and given only superficial requirements.

4.3.6 Requirement documents should not be too large

> "Larger, more complex applications have also traditionally meant larger, more complex requirements specification documents. Yet, as such documents have become larger, they have also become more difficult to understand, review, and use." [26]

The concern with large requirement documents is that the sheer volume of requirements can cause important parts to be missed. The requirement documents must necessarily grow with the size of the system being procured, but it is important to try to keep them at a manageable size. [26] As is the case with how specific a requirement should be, there is no exact answer to the best size of a requirement document. Compressing a document by removing important requirements would be a bad idea, whilst doing it removing duplicate or unnecessary requirements could be beneficial.

4.3.7 Well known standards should be followed

> "The specifications studied very seldom require these [well-known and rigorously reviewed] standards to be followed." [25]

Because of the difficulty in dealing with security, and the importance of doing it right, several international standards exists for secure development of applications, and for security work in organisations. The goal is to help organisations work in a manner that ensures security, and aids in the development of secure products.

The standards in question often define how a security organisation should be established and run, as well as including security in the day-to-day operations of the company. Requiring a supplier to follow such standards helps ensure that security is part of the priorities of the supplier.

4.4 Standards

There exists a set of standards that can be of use in the development of secure software. These standards give advice and guidelines to what requirements should be set in terms of security. If instead the purchaser elects to write their security requirements without the support of any standards, problems, such as missing, weak or irrelevant requirements, are expected [25].

In the following sections *Common Criteria*, *ISO 27002* and *PCI-DSS* will be presented. Common Criteria and ISO 27002 have been selected because of their wide adoption [27, 28], while PCI-DSS is a more detailed and implementation oriented standard that can provide a better insight into the current state of the art of specific requirements.

As stated in the introduction of Common Criteria, it is not meant to be a definitive answer. It is a set of requirements that can be used to create a more secure product. Care needs to be taken in selecting criteria, and it is important to keep up to date with changes. [29] This is true for all standards. In this section, the three mentioned standards will be presented. After this, an attempt to find common categories of requirements that are featured in several of the standards is made. Using these common categories, it will be possible to evaluate if there are certain types of requirements that are commonly recommended by the standards. This is then used in chapter 5 to evaluate the security requirements given in the studied tenders.

4.4.1 Common Criteria

The Common Criteria (CC) [29] is a standard for security certification that allows users and developers to specify respectively requirements and attributes of the system, and lets evaluators determine if the system actually delivers on these claims. [30]

The Common Criteria defines the system that is to be built (and evaluated) as the *Target of Evaluation* (TOE). The evaluation of the system is then done based on three concepts; *Protection Profiles* (PP), *Security Targets* (ST) and *Security Functional Requirements* (SFR). A Protection Profile is an implementation independent set of security requirements, that can be reused for multiple systems. A PP can for example be made for firewalls, and is then relevant for all TOEs that are firewalls. It only includes requirements that are thought to be generic for this class of TOEs. When specifying the exact requirements for a specific product, a Security Target is made. The ST is implementation dependant, and can be based on several PPs, depending on the TOE. The specific Security Functional Requirements are the descriptions for how the system should handle different security situations. One of the strengths of the CC is that it shows dependencies between different SFRs, helping to specify consistent requirements. [31]

The Common Criteria is interesting to look at as it focuses on certifying products, as well as making sure that dependencies are understood and taken into account. At present, it is mostly used to certify smart cards, network products and other IT components [32], but it is also used for pure software products. As such, it is a wide standard, and applicable to most IT related systems and hardware. CC outlines classes that describe a set of security objectives that should be considered when making a risk assessment of the system. The classes are:

- Security audit
- Communication
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Privacy

- Protection of the TOE Security Functionality (TSF)
- Resource Utilisation
- TOE access
- Trusted channels

Common Criteria is publicly available at no cost.

4.4.2 ISO 27002

The ISO 27000-series encompasses a group of ISO standards meant to help keep information secure [33]. The standards are published by the International Organization for Standardization (ISO) and the International Electrotechnical Comission (IEC), supported by national bodies from member countries [34]. The ISO 27000-series includes more than 20 standards, with more than 10 in development [35]. Within the ISO 27000-series, the most relevant standards for this report are the 27001- and 27002-standards.

The 27001-standard is meant to ensure that an organization has the necessary Information Security Management System (ISMS). Following the standard allows for the creation of such a system *"(...) by applying a risk management process and gives confidence to interested parties that risks are adequately managed."* [34]. An ISMS is meant to be used for establishing, operating and improving the information security work in the organization. It allows for a risk based evaluation of the organisation's security needs, and a framework for successful implementation. [36] When acquiring a system, it can be relevant to require the supplier to have ISO 27001 implemented in their organisation. This would ensure that security is central to decisions and the day to day operations of the supplier.

The 27002 standard is a more implementation focused standard, applicable for most systems and organizations, and therefore the one studied in depth in this report. When evaluating which standards to use for a certain system, more specific ISO standards can be of interest. ISO-27002 describes a set of security controls that can be implemented to ensure the security of both an organisation, and an IT-system. A control is defined as a *"measure that is modifying risk"* [36]. In total, 114 controls are defined, though not all will be relevant for all systems. A risk analysis must be conducted, and based on this, appropriate controls can be selected. [37] The 114 controls are sorted into 14 clauses, as given in table 4.1.

The ISO27000-series is available for purchase. At the time of writing, the cost is 2000 NOK[2] from www.standard.no.

Table 4.1: ISO 27002 controls [37]

Security control clause	**Main security categories**	**Control**
Information security policies	Management direction for information security	Policies for information security Review of the policies for information security
Organization of information security	Internal organization	Information security roles and responsibilities Segregation of duties Contact with authorities Contact with special interest groups Information security in project management
	Mobile devices and teleworking	Mobile device policy Teleworking
Human resource security	Prior to employment	Screening Terms and conditions of employment
	During employment	Management responsibilities Information security awareness, education and training Disiplinary process
	Termination and change of employment	Termination or change of employment responsibilities
Asset management	Responsibility for assets	Inventory of assets Ownership of assets Acceptable use of assets Return of assets
	Information classification	Classification of information Labeling of information Handling of assets
	Media handling	Management of removable media Desposal of media Physical media transfer

[2] Approximately $245 at time of writing

Table 4.1 – continued from previous page

Security control clause	**Main security categories**	**Control**
Access control	Business requirements of access control	Access control policy Access to networks and network services
	User access management	User registration and de-registration User access provisioning Management of priviliged access rights Management of secret authentication information of users Review of user access rights Removal or adjustment of access rights
	User responsibilities	Use of secret authentication information
	System and application access control	Information access restriction Secure log-on procedures Password management system Use of privileged utility programs Access control to program source code
Cryptography	Cryptographic controls	Policy on the use of cryptographic controls Key management
Physical and environmental security	Secure areas	Physical security perimter Physical entry controls Securing offices, rooms and facilities Protecting against external and environmental threats Working in secure areas Delivery and loading areas
	Equipment	Equipment siting and protection Supporting utilities Cabling security Equipment maintenance Removal of assets Security of equipment and assets off-premises Secure disposal or re-use of equipment Unattended user equipment Clear desk and clear screen policy

Table 4.1 – continued from previous page

Security control clause	**Main security categories**	**Control**
Operations security	Operational procedures and responsibilities	Documented operation procedures Change management Capacity management Separation of development, testing and operational environments
	Protection from malware	Controls against malware
	Backup	Information backup
	Logging and monitoring	Event logging Protection of log information Administrator and operator logs Clock syncronisation
	Control of operational software	Installation of software on operational systems
	Technical vulnerability management	Management of technical vulnerabilities Restrictions on software installation
	Information systems audit considerations	Information systems audit controls
Communications security	Network security management	Network controls Security of network services Segregation in networks
	Information transfer	Information transfer policies and procedures Agreements on information transfer Electronic messaging Confidentiality or non-disclosure agreements

Table 4.1 – continued from previous page

Security control clause	**Main security categories**	**Control**
System acquisition, development and maintenance	Security requirements of information systems	Information security requirements analysis and specification Securing application services on public networks Protecting application services transactions
	Security in development and support processes	Secure development policy System change control procedures Technical review of applications after operating platform changes Restrictions on changes to software packages Secure system engineering principles Secure development environment Outsourced development System security testing System acceptance testing
	Test data	Protection of test data
Supplier relationships	Information security in supplier relationships	Information security policy for supplier relationships Addressing security within supplier agreements Information and communication technology supply chain
	Supplier service delivery management	Monitoring and review of supplier services Managing changes to supplier services
Information security incident management	Management of information security incidents and improvements	Responsibilities and procedures Reporting information security events Reporting information security weaknesses Assessment of and decision on information security events Response to information security incidents Learning from information security incidents Collection of evidence

Table 4.1 – continued from previous page

Security control clause	**Main security categories**	**Control**
Information security aspects of business continuity management	Information security continuity	Planning information security continuity Implementing information security continuity Verify, review and evaluate information security continuity
	Redundancies	Availability of information processing facilities
Comliance	Compliance with legal and contractual requirements	Identification of applicable legislation and contractual requirements Intellectual property rights Protection of records Privacy and protection of personally identifiable information Regulation of cryptographic controls
	Information security reviews	Independent review of information security Compliance with security policies and standards Technical compliance review

4.4.3 PCI-DSS

Payment Card Industry - Data Security Standard (PCI-DSS) is a standard developed to facilitate the adoption of data security measures in the payment card industry [38]. While it is not meant as a document to cover generic systems, it is interesting to investigate, as the banking and finance world has always been interested in, and been at the forefront of, security. The stakes are high when regularly dealing with billions of dollar, and banks have been targets of hacking since the 1980's [39, 40]. It should then be expected that the requirements set for payment card data will be well thought through.

The PCI-DSS provides much more detailed and implementation specific requirements than Common Criteria and ISO 27002. It is meant to ensure that everyone handling card holder data does so in a secure and consistent manner. As such, the requirements must be easy to understand and implement. [38] Its wide adoption and its connection to the risk averse banking industry, makes the PCI-DSS ideal to study as a set of state-of-the-art recommendations for concrete security requirements.

Substituting the more generic term *data* for *card data*, the main requirements given in PCI-DSS are:

- Install and maintain a firewall
- Do not use vendor-supplied defaults
- Protect stored data
- Encrypt transmission of data across open, public networks
- Protect all systems against malware, and regularly update anti-virus software or programs
- Develop and maintain secure systems and applications
- Restrict access to data by business need to know
- Identify and authenticate access to system components
- Restrict physical access to data
- Track and monitor all access to network resources and data
- Regularly test security systems and processes
- Maintain a policy that addresses information security for all personel

The PCI-DSS is publicly available at no cost.

4.4.4 Common ground

Having studied these three standards, it is desirable to make some recommendations for security requirements that should be included in a requirement specification. Evaluating the tenders studied in this report against all three standards would not be feasible. Instead, areas that are similar in the three standards are identified, and 10 categories of security requirements are presented. These categories, given in table 4.2 and 4.3, give an overview of areas that should be considered when writing security requirements.

There will obviously be situations where some of the areas for requirements presented in the standards are not relevant, and they are not meant to be used as checklists. Both Common Criteria and ISO 27002 states that a risk analysis is necessary before selecting security requirements. However, as most systems developed today are connected to the internet, there will be a lot of requirements that are needed, even for simple systems. Selecting the requirements, or areas of focus, that are repeated in several standards seems a good way to identify important categories of requirements.

From the three standards, we can extract areas where it is reasonable to assume that requirements should be set. These are presented in table 4.2[3]. As the three standards define their requirements in quite different ways, there will be some overlap between categories. To make the categories fit the descriptions in the standards, they have been given broad names. To demonstrate support for the categories, a couple of examples from the standards are given in table 4.2 for each category. In addition, table 4.3 provides an explanation to each category in natural language. Together, table 4.2 and 4.3 presents and explains the categories of requirements that the standards appear to have in common, and which is used in chapter 5 to evaluate the tenders.

Table 4.2: Summary of requirements in standards

Category	**Examples from category**
Cryptography	Encrypt data on open networks * Key management$^{\dagger\ \ddagger}$ 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

[3] The order in which the requirements appear is arbitrary

Table 4.3: Explanation of categories

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.

4.5 Data processor agreement

As a side track from the theory so far, a short dive into the field of data processor agreements. This is an agreement that must be signed by the supplier if the customer's data contains personal information regulated by Norwegian law, and is to be stored outside of the purchasers control. The goal of the agreement is to ensure that the supplier keeps personal information safe, and only grants access to those with legitimate need. [41] Data processor agreements have come into focus lately, when the EU court ruled that transfer of data to so-called *safe harbour* areas was no longer allowed. The areas in question were American organizations that were supposed to live up to European standards for privacy, allowing for the storage of personal information. [42, 43]

It is the responsibility of the *data controller* (the organization that owns the data) to ensure that the data is treated in accordance with the Personal Data Act. When using an external company to process or store the information, a data processor agreement ensures that the *data processor* (the external organisation) handles the data in accordance with the law, and only uses the data for the stated purposes. [41]

There is only a need for a data processor agreement if the data is of a personal nature, as defined in the Personal Data Act, *and* the data is *not* to be processed and stored solely by the data controller. As such, it is not relevant for all tenders.

Chapter 5

State of the practice

This chapter will present an overview of the 29 documents that were retrieved for this project. The tenders have been selected as described in 2.1.1. Most of these were acquired through Doffin, while some were sent to Lillian Røstad on her request.

Section 5.1 gives an overview of the tenders studied in this report, and presents key numbers on competition types, cost estimates and tender distribution between municipal and governmental systems. In section 5.2, the number of security requirements in the studied tenders are presented. The security requirements have been classified according to the categories identified in section 4.4.4. Section 5.3 evaluates how the security requirements in the tenders fulfil the recommendations from the literature, as presented in 4.3. Lastly, section 5.4 discusses the tenders without security requirements, and section 5.5 discusses data processor agreements.

The tenders have been anonymised in this report. There are several reasons for this decision. Firstly, the goal of this report is not to identify specific projects or purchasers that are doing a particularly good or bad job at writing security requirements. Secondly, the documents being reviewed relate to systems that have been, or soon will be, set in production. Should certain systems be pointed at as having bad security requirements, this could be used by people with bad intentions to identify systems that are weak, and potentially launch attacks against them. The tenders that are analysed in the report are presented in appendix A for completeness and reproducibility, but they will not be connected to specific requirements.

Almost all the studied tenders are written in Norwegian. The presented requirements are therefore a translation made by the author. The exact Norwegian wording of translated requirements are given in appendix B under the same heading as in this chapter. Some requirements have been slightly altered to ensure that they can not be connected to a specific tender.

5.1 Overview of selected tenders

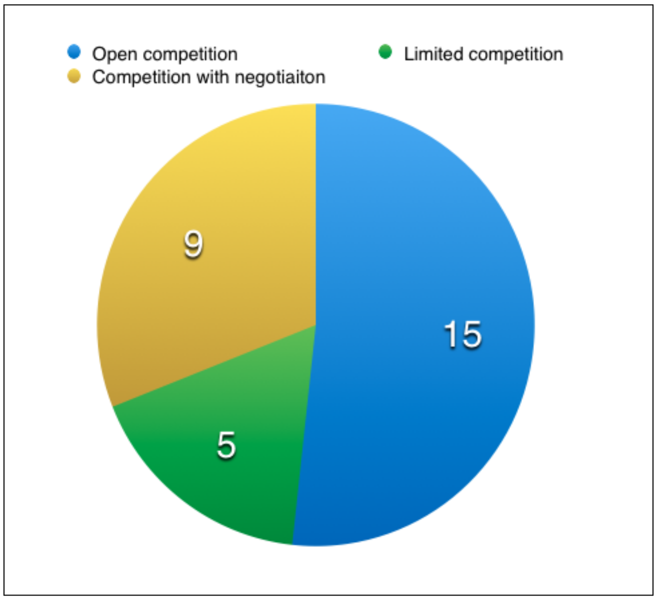

Figure 5.1: Summary of competition types in selected tenders

In total, 29 tender documents were selected for study. Eleven are from municipalities or county municipalities, while the remaining 18 are governmental. 20 of the documents have given an indication of the total expected budget for the system. The average system is expected to cost 26.7 million NOK, although there is one significant outlier in this calculation, the removal of which brings the average down to 10.0 million NOK. 24 of the tenders reviewed are tenders for the purchase of a defined system, while 5 are tenders for the purchase of expertise competence.

The tenders that were selected are distributed between the different competition types described in section 3.3 as shown in figure 5.1. The most common competition in the selection is open competition (15 tenders), followed by competition with negotiation (nine tenders). There are five tenders that are limited competitions. Three of these were acquired through the network of Lillian Røstad. One of the reasons for this type of competition to be more rare might be that most limited competitions are sent out to a set of already pre-qualified suppliers, and is then exempt from publication i DOFFIN.

5.2 Security requirements in selected tenders

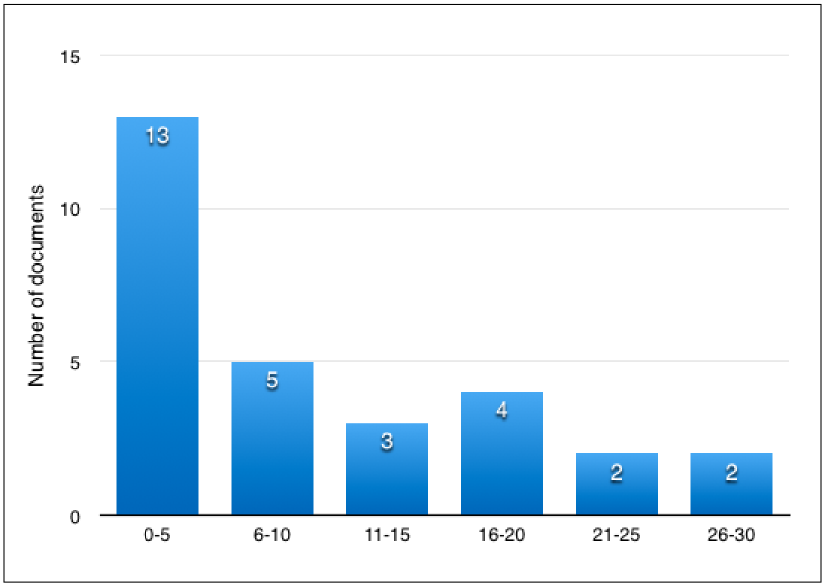

Figure 5.2: Histogram of number of security requirements per system

To give an overview of the state of the security requirements in the tenders, figure 5.2 illustrates how many security requirements are given in each tender by way of a histogram. In the studied tenders, it is most common for there to be between 0 and 5 security requirements. Considering that 10 categories of security requirements were identified in section 4.4.4, having 5 or fewer security requirements seems too little to cover the necessary ground.

Figure 5.3 shows the number of tenders that have at least one requirement in the different categories of security requirements defined in 4.4.4. As is evident, there are no categories for which all tenders have requirements. The most common category for requirements is *authentication of users*, followed by *operations security* and *compliance*. Seeing as user authentication is one of the security features people are most used to dealing with (through login systems), it is perhaps no surprise that this is topping the list.

Requirements for logging is the main reason for *operations security* being high in the list. This might have a relation to the high number of *compliance* requirements, as complying with

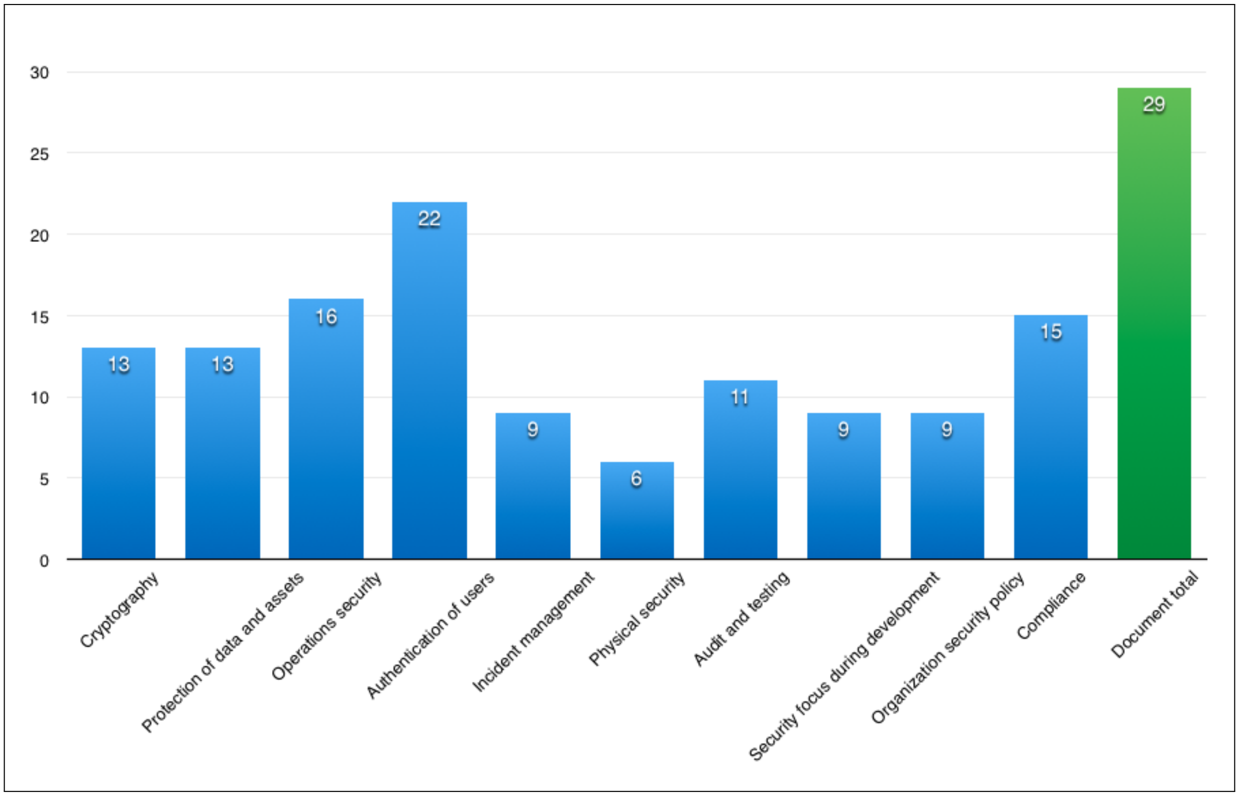

Figure 5.3: Number of tenders with at least one requirement in the given category

many of the relevant laws would be practically difficult without logs. As SINTEF found in their study of information security maturity in Norwegian governmental organisations [44], these organisations are particularly good at compliance. It is reasoned that this has to do with the fact that governmental organisations are used to fulfilling legal requirements, and that many of these organisations have their own lawyers.

The least common category for requirements is *physical security*, with only 6 of 29 tenders making any requirements in the category. This is discouraging, as it would appear that the understanding of security is not good enough in the organizations writing the tenders. Having secure data transfer over the internet is not very useful if the attackers can walk in and grab the servers.

One might expect there to be a correlation between the number of security requirements and the estimated cost of a project. A scatter plot of cost versus number of requirements is given in figure 5.4[1]. There appears to be no correlation between the cost of a system and the number of security requirements that are given in the tender. The figure shows that the cheapest systems have few security requirements, but there are too few systems with a low cost to be able to draw any conclusions.

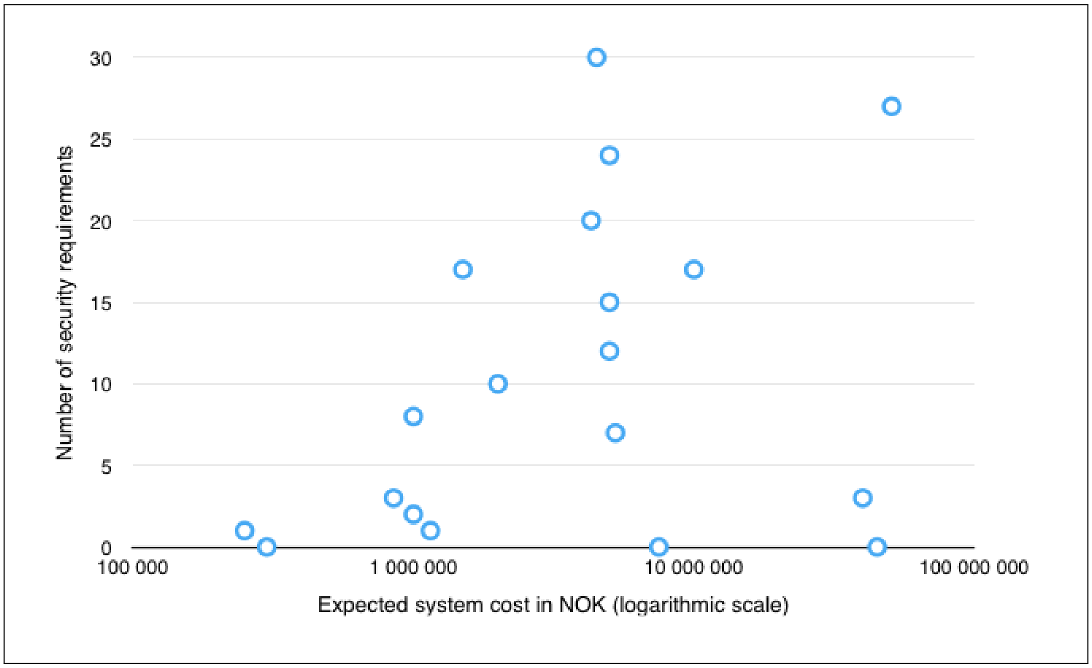

Figure 5.4: Number of requirements plotted against estimated project cost

Another correlation that might be expected is between the total number of requirements for a system, and the total number of security requirements. The rationale being that an organisation that writes an extensive and thorough requirement specification will also make sure to cover most aspects of security. Figure 5.5[2] shows the total[3] number of requirements plotted against the number of security requirements. There appears to be some relation between the number of total requirements and how many security requirements are given. Most systems with more than 100 requirements had at least 10 security related requirements, while almost

[1] 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.

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

[3] Some tenders have optional functionality the supplier may chose 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.

no system with less than 100 requirements had more than 10 security requirements. While the sheer number of security requirements does not imply high quality security requirements, section 4.4.4 shows that there is a lot of ground to cover in the field of security, and as such, a certain number of requirements is needed to capture all aspects of security.

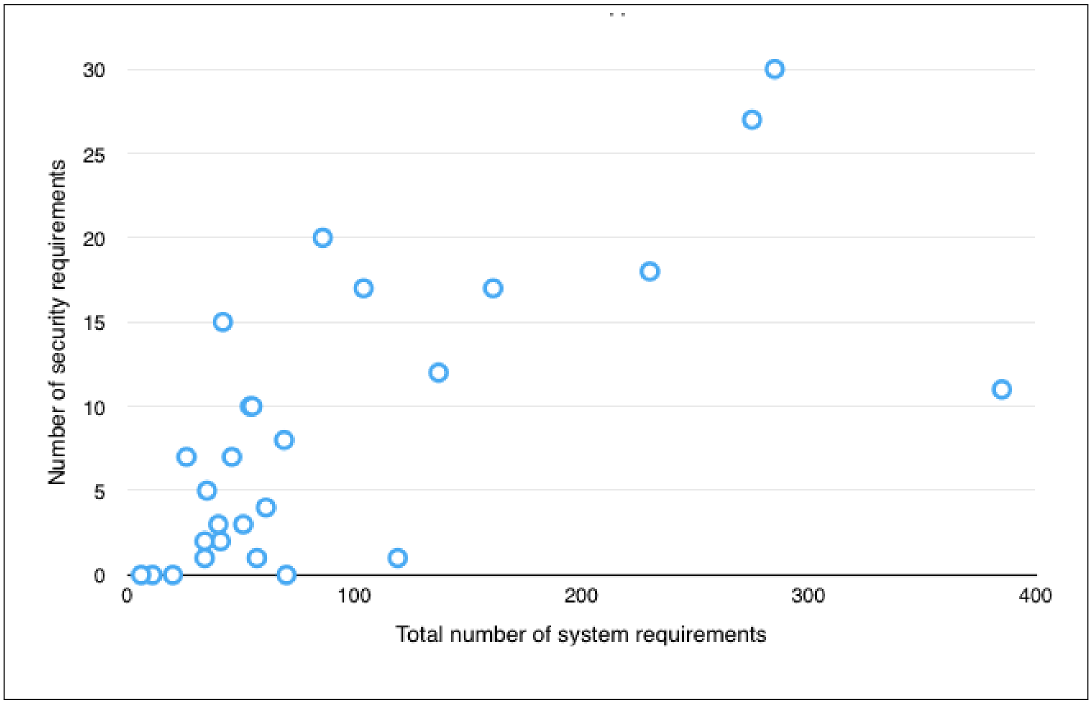

Figure 5.5: Number of requirements plotted against number of *security* requirements

5.3 Recommendations from the literature

In this section, some examples from the tender documents will be given to illustrate the adherence to the recommendations given in the literature, as presented in section 4.3. Generally, each recommendation type is illustrated with one or more examples from the studied tenders, followed by an evaluation of the total state of the studied tenders.

The examples used in this section has been chosen from a wide selection of the tender documents, with the goal to use examples from as many tenders as possible. In addition to the explicit examples given, each section provides a summary of the total state of the studied tenders, and, where possible, a conclusion or recommendation.

A common theme is that there are large differences in how the requirements in the tenders correspond to the recommendations. No single tender appears to have found the *sweet spot* when writing their requirements.

5.3.1 Gather security requirements in one place

The gathering of security requirements varies for the tenders studied, but many attempt to group these requirements in a dedicated section. Returning to the challenge of defining security requirements in section 4.2, there are differences in what is treated as a security requirement. Many tenders that have a section for security requirements also have other requirements that relate to security elsewhere in the specification.

A good illustration of this from the studied tenders is a system that has the following security requirements:

Security

1. "The solution must have the possibility for granular access control from super user level to rights for ordinary users, down to document level."
2. "The solution must use HTTPS in all data communication."
3. "Integrity shall be taken care of such that information in the solution shall ha correct and known quality, and can not be changed by unauthorized users. It shall be possible to trace back when and by whom a change is carried out."
4. "Handling of confidential information."
5. "It is the supplier's responsibility to ensure that web-applications and adaptations are developed and handled in such a way that they do not pose any threat related to confidentiality, integrity and availability, and through this to assure the customer that the solution does not contain potential weaknesses and vulnerabilities.
6. Parts of the information on the new intranet solution must communicate with [company name's] coming intranet."
7. "The supplier is additionally encouraged to offer and describe other functions and properties that are relevant and value increasing."

In addition to this, several requirements that are related to security is found throughout the requirement specification document:

- "Different users must be able to have different rights based on roles. Describe solution."
- "Describe possibilities for access control of users in the publishing solution using Active Directory."

- "Administrator should have an overview over all internal and external users in the intranet, such that access can be controlled and possibly expired users can be removed."

In this case, the first security requirement in the security section pertains to users and user roles. Specifically, it relates to the access each user has to perform actions and view documents. The extra requirements found in the specification also describe users, their access, and the possibility to have them removed. They are placed under the heading *administrative functions* in the requirements document.

In another system, 20 security requirements are given under the section heading *security*. Five other security related requirements were found under the heading *technical requirements*. There are also examples of systems that have made no attempt to gather the security requirements. One system containing 26 functional requirements, where five were identified to be security related, has the security requirements spread throughout the specification.

Most of the tenders that specify a larger number of security requirements have placed the better part of these under its own heading, though some remain under different headings. This is in line with the findings of Lami et.al. [22] who in their analysis also finds there to be misplaced security requirements. As illustrated in the first example in this section, a problem might arise when security requirements related to the same security function are spread across the document. Keeping them consistent as well as making the supplier understand the relation between the requirements might become difficult.

5.3.2 Security requirements should not place unnecessary constraints on the system

It is difficult to draw the line between a requirement that is specific enough, and one that constrains the developers of the system too much. The primary pitfall to an overly constrained requirement is that the purchaser risks getting too specific competence, or a system that can not adapt to changes. Asking for a system that uses HTTPS to transfer data, may stop a supplier using SFTP from delivering what could be a superior system. If the constraint in technology is not done as part of a concious decision based on a real need, but rather is done unintentionally, the restrictions placed on the suppliers can hinder the use of the most appropriate technology, or exclude suppliers with a solution that would have been acceptable.

The first example is a requirement from a tender requesting competence:

- "Security: CheckPoint Firewall with Gaia OS"

There can be several reasons for such a specific requirement. Most likely, the customer uses the given system, and expects to keep using it for the duration of the agreement with the supplier. Should there be changes to the customer's infrastructure however, this requirement might be rendered useless. In that case, the customer would have been better off writing a broader requirement asking for generic knowledge of firewalls, or at least complementing the existing requirement with one for more general competence.

A good example of a more open ended requirement specifies the need for secure transfer. Instead of restricting this to one technology, examples of what can be accepted are given:

- "Secure transfer is to be used when data is exchanged, for instance documents (import and export). E.g. SSH / SFTP / HTTPS etc."

This requirement is in line with the recommendations from the literature. The actual need (secure transfer of data) is presented, and is the subject of the requirement. The implementation specific part is left to the supplier. This requirement is especially good as it also gives examples of technology. This makes the requirement clearer, while not putting any restrictions on the suppliers.

In some cases a constraining requirement is necessary. When national laws or standards are to be followed, there should be no doubt about what standard, and version thereof, is to be used. This is exemplified by the requirement below:

- "The solution must be able to deliver extracts in accordance to Noark 5 standard."

To satisfy relevant laws, the standard given must be followed. As such, this requirement is not *unnecessarily* placing constraints on the development of the system.

When dealing with such constraining requirements, it is important to evaluate if there is a need for a more open version of the requirement. An example would be the following requirement:

- "[In the description, it should be described how:] the solution supports signing of a PDF/A-1 (PDF 1.4) document."

While PDF/A-1 is the standardised PDF-format for long term storage, due to it being more self contained than other versions of the format [45], the customer might have benefited from a more general requirement. What if a new standard for long term storage was announced during the tender process? What if the customer later wanted to sign not only documents meant for long term storage? A requirement stating that *"the solution must support signing of PDF documents, both for long term storage and the most current PDF standard"* might have been more suitable.

The general impression is that most requirements in the studied tenders are not too constraining. Several tenders have very specific requirements in some fields, but this is mostly due to integration with existing systems. Some of these could have benefited from some requirements describing the general technology. This would have allowed for a more flexible system, as well as ensuring that the customer gets a system that can handle future technology development.

5.3.3 Security requirements should not be too open or vague

On the flip side, there are requirements that are too open. They can either be impossible to answer because the supplier is unable to fully understand the need of the customer, or the supplier may be able to deliver a sub-standard solution that the customer must accept.

An example is a requirement for general information security:

- "[The customer] demands that the solution is secure, and ensures integrity, confidentiality and availability of data and systems. Describe how data and systems are secured."

It can easily be claimed by the supplier that the system ensures integrity, confidentiality and availability. There is no good way to verify this claim; the customer must either take the suppliers word for it, or put the system through extensive penetration testing. Asking the supplier to give a description of their security is a step in the right direction, but all descriptions now have to be evaluated against each other. This can be difficult to do objectively, risking the cancellation of the tender.

Answering a tender with this requirement can also be dangerous for the supplier. If the supplier attests that their system *"is secure, and ensures integrity, confidentiality and availability"*, they might be held responsible for this if there are later security incidents. As [19] states: *"Verifying that something is prevented entails proving a negative: that there are no counterexamples."*. This is close to impossible, and not something that can be expected of a supplier to either implement, nor prove.

Other requirements used vague qualitative statements:

- "Good spam and phising filter"
- "It is desired that the supplier offers consultants with the best possible experience from security testing."

These requirements contain qualitative words such as *good* and *best.* As discussed in Lami et.al. [22], it is difficult to evaluate requirements containing these kinds of words. What is considered "good spam filtering" will be grounds for interpretation, and as such, both the customer and supplier might be able to claim that the other is in the wrong.

In some cases, some of the only security requirement given were extremely vague.

- "In addition, there will be a need for competence on surrounding subject areas such as security on source code level."

It should be noted that this requirement is from a tender for competence, and as such, the specific system to be built is not specified. Despite of this, requesting such broad competence will most likely not lead to suppliers offering their top security people, as fulfilling the requested competence can probably be done with junior staff.

In the 29 studied tenders, the use of the word "good" in relation to security requirements is not uncommon. A pattern that emerges is that tenders using "good" and other qualitative statements in one requirement, repeat this in several other requirements.

One example of this is from a tender that gives the following requirements:

- "The supplier shall have good measures against hacking of the service."
- "The supplier shall have good measures against loss or exposure of logs (logins, reading/writing of data etc.)"

- "The supplier shall have good measures against unauthorized access to premisses, machines, backup etc."

It is difficult to determine what measures against hacking are "good". Should they not be "great"? How do we know they are not just "okay"? Interestingly, the tender in question is one of the few covering almost all the categories of security requirements defined in 4.4.4. It would appear that great care has been taken in covering all aspects of security, but the requirements written may be too vague to ensure that the wanted level of security is accomplished.

Several of the studied tenders use qualitative statements in their security requirements. This should be avoided, as it makes the requirements difficult, if not impossible to evaluate. Security requirements must be written in a manner that can be measured objectively to avoid simple solutions that does not mitigate security risks, but are still in line with the given system specification.

5.3.4 There should be a consistent selection of security requirements

Looking at figure 5.3, the situation described by Wilander and Gustavsson [25] seems to emerge. They point to the fact that if requirements for access control are given, but no requirements for encryption or physical security are present, there is an inconsistency as the first requirement indicates that securing data is important, but that would entail the need for encryption and physical security.

In the studied tenders, there are 22 systems that have some sort of requirement for user authentication, while only 13 systems have requirements regarding cryptography. Physical security is only mentioned in 6 of the studied documents. This supports the findings of Wilander and Gustavsson [25], and shows that there is a lack of consistency in what requirements are set.

One of the studied systems provides the following requirements related to user authentication and roles:

- "The Contractor is asked to describe how the user access is administered in the system."
- "The Contractor is asked to describe the access control management."
- "[Functionality of the system] should also be accessible over a secure, closed web solution."

Other than this, there are also a number of requirements for up-to-date antivirus and patching of the system. This paints a picture of a system that contains important information that should not become available to others. In contrast to this, the most relevant security requirement to encryption and physical security is:

- "[The customer] wants the Contractor [to] manage security and work processes related to service delivery in a professional manner."

This is a representative example of the state of many of the studied tenders. It appears that few of the tenders have written their security requirements based on a understanding of the risks facing the system, but have rather gathered a set of security requirements that seemed to be fitting. This underlines the importance of the risk assessment recommended by the standards studied in section 4.4. Without knowledge about the risks facing a specific system, and the assets contained within, it is difficult to write a set of consistent requirements.

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

An inconsistency of detail can be found in several of the tenders. One tender has 13 requirements for user authentication, while the other categories have from 0 to 4 requirements. In total, 27 security requirements were identified in this tender, and almost half of these focus on user authentication. While we have seen that it is not unusual for user authentication requirements to make up the better part of requirements, this can also be due to the local heroes described by Willander and Gustavson [25].

Interestingly, this example can also be used to illustrate the findings in section 5.3.4. The described system has no requirements for cryptography, and few requirements concerning secure development and operations security. If the skewness of the requirements is due to a local hero, this might suggest that the entire picture of security is not captured by a person who mostly champions a single area.

It is difficult reach a conclusion for this recommendation. More than 2500 system requirements are part of the tenders studied, and most of the focus has been on the security requirements. Making an assessment of whether the security requirements are more or less detailed than the rest of the requirements is a task that, due to time, falls outside the scope of this report. Comparing only security requirements within the same tender, some categories are found to have significantly more requirements than others. It does however appear that individual security requirements of different categories, within the same tender, has a consistent level of detail.

5.3.6 Requirement documents should not be too large

Size of the requirement documents has perhaps been one of the most varying factors between the studied tenders. One of the smallest systems was described in full with only six *functional* requirements, while the larger systems had hundreds of requirements spread over several documents, with 385 requirements being the maximum.

The importance of this recommendation is mostly to ensure that the documents do not grow out of control. It is understandable that the customer might want to be very explicit with requirements in a tender process, to ensure that the system developed is actually the one that is wanted. This is also one of the recommendations in this report. It must however not be interpreted as a reason to write enormous requirement documents. Not only would they be harder to read for the suppliers, but the risk of inconsistencies arising increase with the document size.

One of the tenders with the most requirements had more than 280 system requirements in total, spanning three separate agreements for development, operations and maintenance. The security requirements are somewhat drowned out by the sheer size of the documents. For the sake of clarity: the system in question is estimated to cost well below the average of the studied tenders, and has security requirements in most of the categories defined in 4.4.4. This demonstrates that system cost is not necessarily connected with the number of security requirements, as corroborated by figure 5.4.

While ensuring that the requirement documents are kept at a manageable level, figure 5.5 shows that requirement documents with more requirements are likelier to include more security requirements. While it is not the *number* of security requirements that decide if security is well thought through, we have seen that many sides of security must be taken into account, and this can not be done in just a few requirements. Due to this, it is difficult to conclude that purchasers should limit the size of the requirement specifications, but care should be taken to make sure they are not larger than necessary.

5.3.7 Well known standards should be followed

As discussed in section 4.4, a number of standards exists in the field of information security. These are not intended to be used uncritically, nor should all recommendations be followed by all systems, but seeing as almost all the systems studied in this report has some connection to the internet, they can be a useful starting point.

Table 5.1: Tenders with no requirements for following standards

Number of tenders	No standards requirement
29	18

As shown in table 5.1, 18 of the studied tenders had no requirement for the suppliers to be certified in, or follow, any standards in their work. The tenders that did include such requirements used a broad spectre of standards. Some used internally developed guidelines based on, among other things, well known standards, others referenced guidelines published by the Norwegian National Security Authority (NSM). Standards from the ISO 27000 family are the most common standards referenced. In addition to this, several tenders reference the OWASP Top 10, a list of the ten most central risks facing web applications [46].

Several of the tenders that do not excplicitly reference any standards have nevertheless included requirements that are meant to make the suppliers use some framework or standards.

- "Document the infrastructure and security solutions for the suggested [solution], which must be in accordance with current standards for system architecture and security."
- "The supplier shall use the highest relevant industry standards for secure software development to discover and solve critical security problems as fast as possible. "Highest relevant industry standards" shall be understood as the degree of accuracy, knowledge, efficiency and diligence that a diligent person with technical expertise in the area and under corresponding conditions would operate under."

The main problem with these kinds of requirements is how to interpret and implement them. What are "current" or "relevant" industry standards? The second requirement makes an effort to explain this, but the explanation leaves as many new questions as it answers. How is a developer supposed to act as an expert in the field, unless the person is already an expert? What constitutes a diligent person, and how can we know how he or she would act? All in all, these kind of requirements add little to the security requirements. The possibly only effect they have is to act as a legal shield for the purchaser, and a deterrent to answering the tender for suppliers.

5.4 Documents without security requirements

Of the studied tenders, 4 did not provide any requirements related to security, and 3 provided only one. What, and how much, to demand in terms of security is always something that must be evaluated for each individual system. However, it seems unlikely that so many tenders relate to systems so isolated, and operated by personnel so trusted, that (virtually) no security requirements are necessary. Should this be the case, one might expect the tender to describe the system's use as limited to secure internal networks. This is however not the case in the tenders studied, which raises the question if security has been thought of at all.

There are some plausible explanations to why this is the case. Some of the mentioned tenders use a competition form that allows for negotiation. The customer may have planned to bring up security later in the process, and to speed up production of the tender documents, left security out. If the purchaser knows that the system they are acquiring will be based on a standard system (known as *Commercial off the shelf*) they might assume that security is built in, and only specify special use cases and requirements for their organization.

Opting to not give any security requirements is highly advised against. At a minimum, a risk analysis should be conducted, and a basic set of security requirements included in the requirement specification. Failing to do so leaves security up to the supplier, and might cause the final product to have serious security holes.

5.5 Data processor agreements

In the tenders studied, 6 had either attached a data processor agreement to be signed by the suppliers, or set a requirement for such an agreement to be signed. One supplier had a requirement for an agreement to be signed "if needed". It should be noted that when requesting the tender documents, not all purchasers returned the full set of documents, only the ones seen by the purchaser as relevant to the report. Because of this, it is possible that more tenders had a data processor agreement attached to the tender documents.

As stated in section 4.5, data processor agreements are not relevant for all studied tenders, and it is not expected that all tenders would require a data processor agreement. For several of the tenders in the study, it is either not clear where data will be stored, or this is something the supplier is asked if they can provide, though it is not set as an obligatory requirement for selection.

Looking into data processor agreements was done in the hope of being able to say something about the use of the agreements, how they are specified, and perhaps if they are required in all situations where it would be appropriate. It has proven difficult to identify if a system would need such an agreement. Given this, as well as the fact that not all documents for all tenders could be reviewed, no conclusion on the subject can be reached.

Chapter 6

Conclusion

In section 1.2 three research questions for this project thesis were set forth. In this chapter an answer to the questions will be given. The literature recommendations will be summarized, as well as compared to the actual requirements in the studied tenders.

6.1 Literature recommendations

Research question **RQ2** relates to the state of the art on security requirements. Chapter 4 outlines the current recommendations for writing security requirements, and identifies 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 to 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 to this, the ISO-27002 standard, Common Criteria and PCI-DSS standards where analysed, and a common ground of 10 categories from the standards was 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

6.2 Requirements in studied tenders

RQ1 asks what security requirements are set in tenders, and **RQ3** pertains to how this corresponds with literature recommendations. Section 5.1 and 5.2 gives an overview of the requirements provided in the studied tenders. There is great variety in what categories security requirements are set, how many security requirements are given, and if use of standards are required.

As shown in section 5.3, the correspondence between the literature recommendations and the current state of the art is varied. While there are many examples of poor security requirements, there are also tenders that present well written and balanced security requirements.

Gathering security requirements

Most of the purchasers who have a significant number of security related requirements gather these in one place. There are usually some security requirements that are placed elsewhere in the specification. This might be because of the unclear definition of a security requirement, or because these requirements describe important functionality, such as authentication and sign-on, which the customer views more as a function of the system than a security feature. Repeating requirements in several sections would probably only lead to confusion, but it might be a good idea to reference where to find all security related requirements in the security section.

Specificity of requirements

The findings in section 5.3.2 and 5.3.3 show that the balance between requirements that are too open and too constrained is very difficult. The customer can be faced with the choice of risking a bad system (because of too strict requirements), or the wrong system (because of too open requirements). Providing alternatives or examples of what is desirable is one solution to this problem. It is also possible to request both general and specific knowledge when acquiring competence. This is in line with the recommendations of Lausen in his discussion on different styles of usability requirements. Supplying a combination of the different styles enables the purchaser to communicate clearly their wishes, and at the same time allows some flexibility for the supplier. [47]

Consistency

Section 5.3.4 and 5.3.5 shows that there are consistency problems in the studied tenders. Purchasers does not appear to recognise the implications a security requirement in one area has on requirements that should be set in other areas. Within the same requirement specification, purchasers appear to write security requirements at a consistent level of detail, at least for the categories of security requirements that are covered.

Document size

As shown in section 5.3.6, and in figure 5.5, the size of the documents studied varied greatly. One of the recommendations from the literature is to keep documents at a manageable size, though the data from this study shows a correlation between the total number of requirements and the number of security requirements (implying that larger documents contain more security requirements). As underlined multiple times, the number of security requirements in itself is not a hallmark of good security, but there is a lot of ground to cover in terms of security, necessitating a minimum of security requirements. The main recommendation is to keep the document size under control, but not sacrifice security requirements for document size.

Use of standards

18 of the 29 tenders studied have no requirements for standards to be used in development. Of the ones that do, several reference internal guidelines, or only standards required by law for specific parts of the system. There are also several tenders using open statements about *relevant industry standards* or similar. These kinds of statements are impossible to verify, and

probably do not contribute to better security. The literature strongly recommends the use of internationally recognized standards to ensure security requirements are consistent and cover all sides of security.

6.2.1 Recommendation gap

In summary, writing requirements that are in line with the recommendations in the literature is a difficult, sometimes impossible, balancing act. Making sure that all requirements are covered in a short and concise document, where no requirement is too open or too restricting is probably not possible, nor something to aim for. As with all matters of security, an individual assessment of the different projects must be done, and based on this some sacrifices must be made. It is however not a bad idea to clarify this in the requirement specification, making the suppliers aware that thought has gone into the choice between competing factors.

Most troubling is the low number of tenders that appear to have used any known standards when defining the security requirements for the system to be acquired. As demonstrated in this report, and well known in the information security community, writing security requirements is difficult. This should be reason enough for a purchaser to find one or more standards to help in the creation of requirements. The Common Criteria provides dependencies between different requirements to ensure that inconsistencies does not arise. ISO 27002 gives more than 100 possible controls, and guidance for implementation. PCI-DSS is a more straight forward standard with 12 simple but vital categories that together gives data protection on the level credit card issuers approve and expect. These standards have gone through many revisions, and are written and contributed to by some of the best security professionals in the business. Implementing one or more of them will be a major step towards custom, consistent, and risk based security requirements, that ensure the security of both systems and data. Using some recognised standard should be seriously considered by all purchasers of IT-systems and services. Attempting to "reinvent the wheel" is unnecessary and inefficient.

While there are no tenders that implement requirements following all recommendations, there are certainly tenders that overall have much higher quality security requirements than others. There does however not appear to be any connection between a high quality security requirement specification and system size, cost, or organisation size or type. Some correlation between the total number of requirements and the number of security requirements is found. Together, this would suggest that local factors are deciding in how well the recommendations for security requirements are followed. The "local hero" theory from Willander og Gustavson [25] is a plausible explanation. This "local hero" may be a single security focused employee, or a small security organisation within the organisation. This would explain why, for example, some municipalities are better at security than large government bodies.

Security is difficult, but must not be ignored. With the continuing digitalization of public services, governmental organisations must improve the security requirements given in tenders to ensure that data and privacy are kept safe.

6.3 Possible weaknesses

While care has been taken to ensure that the work in this report is accurate and correct, there is always room for errors and misunderstandings. In this section, sources of weaknesses are discussed. These should be taken into account when interpreting or using the results from this report.

6.3.1 Selection of tender documents

As mentioned in section 2.1.1, the selection process conducted in this study has been, at best, semi-systematic. The documents were not chosen based on objective criteria, but rather on the basis of interest and the sector involved.

Four of the documents were not acquired trough a search in Doffin, but rather as an answer to a call for documents that Lillian Røstad issued to a selection of people working with IT-security in the public sector. This could have introduced two main sources of bias. The first is the selection of people who received the call for documents. The call was not sent to all security operatives in the public sector. The recipients could have been those deemed most likely to answer, the ones that had a good relation with Røstad, or similar.

The other kind of bias is who elected to answer, and what kind of documents they supplied. Knowing that a system might not have had the best security requirements, one could have elected not to answer, or just to send the most successful projects.

6.3.2 Understanding of the law

While the author has done quite a large amount of research into the laws and regulations that govern the field of public procurement, the author is not a lawyer, nor a law student. The consequence of this is that some finer details of the law may have been foregone, and as such, some conclusions may be rendered invalid.

6.4 Application outside Norway

The analysis in this report are based on Norwegian procurement and, as stated in chapter 3, on the Norwegian regulations in the area. As laws and regulations are usually quite different across countries, research based on this can be difficult to make use of in other jurisdictions. Because of Norway's participations in the European Economic Area however, procurement over the EU threshold follows the same regulation in all EU/EEA-countries. As such, the research in this report pertaining to the legal part of the tender process should be applicable in other EU/EEA-countries.

The findings on security requirements given in tenders should not be uncritically applied to other countries. Differences in business norms, education systems, work stock, and many other factors should be taken into account. It would be interesting to see similar research done on tenders published in other countries.

6.5 Further work

This report has presented findings on the state of the art of security requirements, and the state of practice of security requirements in Norwegian tenders. The research, while interesting in it self, would benefit from further research in surrounding areas. This section presents suggested themes for future research.

6.5.1 Requirement elicitation phase

This report has focused on requirements in systems that are under development, or has already been delivered. We have seen that there is a significant gap between recommendations in the literature, and the security requirements given in the studied tenders. It would be of interest to understand how security requirements are decided upon, and why certain choices are made. A study, using interviews or surveys to look into the process of creating requirement specifications for tenders, would provide interesting insight in this field and the reasoning behind today's state of practice.

6.5.2 Fulfilment of requirements

The interpretation of given requirements by the suppliers is important in the tender process. This will decide if the supplier believes they are able to answer the tender, and if so, what kind of system they believe the customer wants. Research into the supplier side of tender processes, focusing on interpretation and the subsequent fulfilment of security requirements, would contribute to understanding of the complete tender process, and how it affects security.

6.5.3 Other countries

As mentioned in 6.4, it would be interesting to see similar research done in other EU/EEA-countries. There is nothing to suggest huge differences between these countries, especially given the fact that the same laws and regulations are implemented for most procurements. With that said, other factors such as social and cultural may have significant impact.

It would also be interesting to see results from similar studies outside the EU/EEA. Together with studies from within the EU/EEA, this could reveal whether the current procurement system facilitates good requirements, and if the legal framework trumps different social and cultural differences.

6.5.4 Automatic evaluation

The work of Lami et. al. [22] shows the potential of automatically recognizing, classifying and evaluating requirement documents. Building a system that could identify either specific security requirements that can be problematic, or that can analyse the entire document and rate readability, or even quality, of the security requirements could dramatically improve the current situation. With advancements in natural language processing, and the large number of IT-systems being procured, this could be of great interest.

Bibliography

[1] (2006, apr) Forskrift om offentlige anskaffelser - §2-1 (2). [Online]. Available: http://lovdata.no/forskrift/2006-04-07-402/\T1\textsection2-1

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

[3] (2012, Jan) Her er it-norges 100 mektigste. Computer World. [Online]. Available: http://www.cw.no/artikkel/offentlig-sektor/her-it-norges-100-mektigste

[4] “Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova),” may 2006.

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

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

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

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

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

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

[11] (2006, apr) Forskrift om offentlige anskaffelser - §14-2. [Online]. Available: http://lovdata.no/forskrift/2006-04-07-402/\T1\textsection14-2

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

[13] ——. (2015, Nov) Konkurransepreget dialog ved innovative anskaffelser. [Online]. Available: http://www.anskaffelser.no/prosess/innovasjon/innovasjon-steg-steg/gjennomfore-konkurranse/valg-av-prosedyre/konkurransepreget

[14] ——. (2015, Nov) Anskaffelsesprosessen. [Online]. Available: http://www.anskaffelser.no/prosess/anskaffelsesprosessen

[15] (2015, Nov) Avgjorte saker. KOFA. [Online]. Available: http://www.kofa.no/no/Avgjorte-saker/

[16] 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

[17] 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.

[18] 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

[19] C. B. Haley, R. Laney, J. D. Moffett, and B. Nuseibeh, "Security requirements engineering: A framework for representation and analysis." *IEEE Transactions on*

Software Engineering, vol. 34, pp. 133–153, Jan./Feb. 2008. [Online]. Available: http://oro.open.ac.uk/10058/1/01435458.pdf

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

[21] 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.

[22] 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.

[23] S. Lauesen, "Experiences from a tender process," in *Proceedings of REFSQ'04*, 2004, pp. 29–46.

[24] C. Pettijohn and Y. Qiao, "Procuring technology: Issues faced by public organizations," *Journal of Public Budgeting Accounting and Financial Management*, vol. 12, pp. 441–461, 2000.

[25] J. Wilander and J. Gustavsson, "Security requirements–a field study of current practice," *Symposium on Requirement Engineering for Information Security (SREIS'2005), Paris, France*, 2005.

[26] D. G. Firesmith and F. Consulting, "Modern requirements specification," *Journal of Object Technology*, vol. 2, no. 1, pp. 53–64, 2003. [Online]. Available: http://www.jot.fm/issues/issue_2003_03/column6.pdf

[27] (2015, Nov) The iso survey of management system standard certifications. [Online]. Available: http://www.iso.org/iso/news.htm?refid=Ref1686

[28] (2015, Nov) Common criteria certified products list - statistics. [Online]. Available: https://www.commoncriteriaportal.org/products/stats/

[29] (2015, oct) Common criteria. [Online]. Available: https://www.commoncriteriaportal.org/

[30] D. Mellado, E. Fernández-Medina, and M. Piattini, "A common criteria based security requirements engineering process for the development of secure information systems," *Computer Standards & Interfaces*, vol. 29, no. 2, pp. 244 – 253, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0920548906000511

[31] N. Mead. (2013, jul) The common criteria. Carnegie Mellon University. [Online]. Available: https://buildsecurityin.us-cert.gov/articles/best-practices/requirements-engineering/the-common-criteria

[32] (2015, Nov) Certified products. [Online]. Available: http://www.commoncriteriaportal.org/products/

[33] (2015, Nov) ISO/IEC 27001 - Information security management. [Online]. Available: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[34] ISO, "Information technology— security techniques — information security management systems — requirements," International Organization for Standardization, Geneva, Switzerland, ISO 27001-2012 2:2013, 2013.

[35] (2015, Nov) Standards and projects under the direct responsibility of iso/iec jtc 1/sc 27 secretariat. ISO. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306

[36] ISO, "Information technology— security techniques — information security management systems — overview and vocabulary," International Organization for Standardization, Geneva, Switzerland, ISO 27000-2014, 2014.

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

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

[39] M. Saylor, "Evolution of the cyber attack," 2011. [Online]. Available: http://www.isacantx.org/Presentations/2011-05%20Lunch%20-%20Evolution%20of%20Cyber%20Attacks.pdf

[40] (2000) A history of hacking. St. Petersburg Times. [Online]. Available: http://www.sptimes.com/Hackers/history.hacking.html

[41] Datatilsynet. (2015, Nov) Data processor agreements. [Online]. Available: https://www.datatilsynet.no/English/Publications/Data-processor-agreements/

[42] ——. (2015, Nov) Hvordan overføre personopplysninger til utlandet etter safe harbor. [Online]. Available: https://www.datatilsynet.no/Regelverk/Internasjonalt/Hvordan-overfore-personopplysninger-til-utlandet-etter-Safe-Harbor/

[43] ——. (2015, Nov) Safe harbor - prinsipper om overføring av opplysninger til usa. [Online]. Available: https://www.datatilsynet.no/Regelverk/Internasjonalt/Overfoering/Safe-Harbor-prinsippene/

[44] M. G. Jaatun, I. A. Tøndel, and D. S. Cruzes, "Modenhetskartlegging av programvaresikkerhet i offentlige virksomheter," SINTEF, Tech. Rep., 2015.

[45] (2005) New iso standard will ensure long life for pdf documents. ISO. [Online]. Available: http://www.iso.org/iso/home/news_index/news_archive/news.htm?refid=Ref974

[46] (2015, Nov) Owasp top 10. Open Web Application Security Project. [Online]. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[47] S. Lauesen, "Usability requirements in a tender process," in *Computer Human Interaction Conference, 1998. Proceedings. 1998 Australasian*, Nov 1998, pp. 114–121.

Appendix A

Overview of studied tenders

In the work with this report, a total of 29 tenders have been analysed. In table A.1 the organisation issuing the tender, as well as the name of the product or service being acquired is given. All tenders that were found using Doffin have their Doffin reference number supplied.

Table A.1: Tenders analyzed

Organization	Description	Norwegian description	Doffin reference
Bærum Kommune	Individual plan	Individuell plan	-
Bergen Kommune	Broadband routers	Bredbåndsrutere	-
Bergen Kommune	Archive system	Arkivsak	-
Direktoratet for økonomistyring	Reporting tool	Rapporteringsverktøy	2015-124319
Domstoladministrasjonen	Portal solution	Portalløsning	2015-163871
Forsvarsbygg	Booking system	Bookingsystem	2015-130821
Fredskorpset	Project handeling solution	Prosjekthåndteringsverktøy	2015-186382
Gjøvik Kommune	School administration system	Skoleadministrativt system	2015-198853
Helsedirektoratet	Consulting services	Konsulenttjenester	-
Meterologisk institutt	Cloudbased co-operation solution	Skebasert samhandlingsløsning	2015-195710
Molde VGS	Point of sales system	Kassasystem	2015-152546
MuseumsIT	Electronic archive	Elektronisk arkiv	2014-302620
Nord-Trøndelag Fylkeskommune	Resource portal	Resursportal	2015-142585
Nord-Trøndelag Fylkeskommune	ICT equipment and consulting services	IKT-utstyr og konsulenttjenester	2014-151818
Norsk Tipping	CRM system	CRM system	2015-199590
NRK	NCS	NCS	2015-587411
NTNU	E-learning system	E-læringssystem	2014-359391
Politiets Fellestjenester	Consultant services, development and renewal	Konsulenttjenester, utvikling og fornying	2015-897777
Porsgrunn Kommune	CRM	CRM	2015-168694
Ruter	Contract administration system	Kontraktsadministrasjonssystem	2015-125576
Sør-Trøndelag Fylkeskommune	ICT consultant services	IKT-konsulenttjenester	2015-719398
Statens legemiddelverk	Side effekt databse	Bivirkningsdatabase	2014-678880
Stavanger Kommune	Situation maps	Situasjonskart	2014-934476
Trondheim Kommune	Registration and archiving solution	Registerings- og arkiveringslønsing	2015-190340
UngdomsOL	Website	Nettsider	2015-996270
Utenriksdepartementet	Booking system for passport issuing	Bookingsystem for passutsteding	2015-134337
Statens Vegvesen	IPS/IDS	IPS/IDS	2015-162688
Statens Vegvesen	Storage/Backup	Lagring/Backup	2015-749280
Vitenskapskommiteen for mattrygghet	Intranet	Intranett	2015-192501

Appendix B

Translated requirements

The requirements referenced in this report are mainly given in Norwegian, and were translated by the author. To ensure verifiability, the original Norwegian text of the requirements are reproduced in this appendix. Requirements that were given originally in English are not repeated here.

B.1 Gather security requirements in one place

1. Løsningen må ha mulighet for granulær tilgangsstyring fra superbrukernivå til rettigheter for vanlige brukere, ned på dokumentnivå.
2. Løsningen må benytte https i all datakommunikasjon.
3. Integritet skal ivaretas slik at informasjon i løsningen skal ha riktig og kjent kvalitet, og ikke kunne endres av uautoriserte brukere. Det skal være mulig å spore tilbake når og av hvem en endring er foretatt.
4. Håndtering av konfidensiell informasjon
5. Det er leverandørens ansvar å sørge for at web-applikasjoner og tilpasninger er utviklet og håndtert på slik måte at de ikke utgjør noen trussel relatert til konfidensialitet, integritet og tilgjengelighet, og derigjennom å forsikre Kunden at løsningen ikke inneholder potensielle svakheter og sårbarheter.

6. Deler av informasjonen på ny intranettløsning må kommunisere med [kundens] kommende internett.
7. Leverandøren oppfordres i tillegg til å tilby og beskrive øvrige funksjoner og egenskaper som er relevante og verdiøkende.

- Ulike brukere må kunne ha ulike rettigheter basert på roller. Beskriv løsning.
- Beskriv muligheter for tilgangsstyring av brukere i publiseringsløsningen ved bruk av Active Directory.
- Administrator bør ha oversikt over alle interne og eksterne brukere i intranettet, slik at tilganger kan styres og eventuelt utgåtte brukere fjernes.

B.2 Security requirements should not place unnecessary constraints on the system

- Sikkerhet: CheckPoint Firewall med Gaia OS
- Det skal benyttes sikker overføring ved utveksling av data eksempelvis dokumenter (import og eksport) Eks. SSH / SFTP / HTTPS etc.
- Løsningen skal kunne avlevere uttrekk på Noark 5-standard.
- [I beskrivelsen skal det også fremkomme om/hvordan:] løsningen støtter signering av et PDF/A-1 (PDF 1.4) dokument

B.3 Security requirements should not be too open or vague

- [Kunden] krever at løsningen er sikker, og vil ivareta integritet, konfidensialitet og tilgjengelighet på data og systemer. Beskriv hvordan data og systemer er sikret.
- Det er ønskelig at tilbyder kan tilby konsulenter som har best mulig erfaring fra sikkerhetstest.
- I tillegg vil det være behov for kompetanse på omkringliggende fagområder som sikkerhet på kildekodenivå

- Leverandøren skal ha gode tiltak mot hacking av tjenesten.
- Leverandøren skal ha gode tiltak mot tap eller eksponering av logger (pålogginger, lesing/skriving av data, m.m.)
- Leverandøren skal ha gode tiltak mot uatorisert tilgang til lokaler, maskiner, backup osv.

B.4 Well known standards should be followed

- Dokumentere infrastrukturen og sikkerhetsløsningene for foreslått [lønsning], som må være i henhold til gjeldende standarder for systemarkitektur og sikkerhet
- Leverandøren skal benytte de høyeste relevante industristandarder for sikker programvareutvikling for å oppdage og løse kritiske sikkerhetsproblemer så raskt som mulig. ”Høyeste relevante industristandarder” skal forstås som graden av nøyaktighet, kunnskap, effektivitet og aktsomhet som en aktsom person med teknisk ekspertise på området og under tilsvarende forutsetninger ville operere etter.