Information Security Requirements in Public IT Procurements

Effect of Act on Information Management in Public Administration on Requirements

Riina Aaltonen

Master's thesis
May 2020
Technology
Degree Programme in Information and Communication Technology
Master's Degree Programme in Cyber Security

jamk.fi

Description

Author(s) Aaltonen, Riina	Type of publication Master’s thesis	Date May 2020
		Language of publication: English
	Number of pages 70	Permission for web publication: x

Title of publication

Information Security Requirements in Public Procurements

Effect of Act on Information Management in Public Administration on Requirements

Degree programme

Degree Programme in Information and Communication Technology, Cyber Security

Supervisor(s)

Huotari, Jouni; Hautamäki, Jari

Assigned by

Legal Register Centre; Lehtisalo Mikko

Abstract

Public authorities have started to digitalise their services based on the key project ‘Public services will be digitalised’ by the Government Programme of former Prime Minister Juha Sipilä's government. The renewal of the information management legislation was also included in this same programme. The current Act on Information Management in Public Administration entered into force 1 January 2020 and has also provisions on information security that affect public IT procurements.

There were three objectives in the research. The first objective was to study the change in the Finnish legislation regarding information security requirements in public IT procurements. The second objective was to study what the different aspects for information security requirements were in public IT procurements or if there was only one viewpoint. The third objective was to study what a well-formed requirement is.

The used method was content analysis consisting of the interpretation of the law. The legislation under research was analysed and applied against the general principles of secure coding and other methods and best practices.

It was found out that there are three kind of information requirements in public IT procurements: for the authority defining the subject-matter of the procurement, for the supplier to guide service production and for the production of service output and detailed requirements for implementation of the service output.

The information security requirements in public IT procurements should be customised. Their definition needs to be part of the total definition of subject-procurement because there are dependencies between information security issues and other issues.

Keywords/tags (subjects) authorities, data security, , information management, information security, legislation, public procurement, requirements engineering, software development

jamk.fi

Kuvailulehti

Tekijä(t) Sukunimi, Etunimi Aaltonen, Riina	Julkaisun laji Opinnäytetyö, ylempi AMK	Päivämäärä Toukokuu 2020
	Sivumäärä 70	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Information Security Requirements in Public Procurements

Effect of Act on Information Management in Public Administration on Requirements

Tutkinto-ohjelma

Degree Programme in Information and Communication Technology, Cyber Security

Työn ohjaaja(t)

Jouni Huotari; Jari Hautamäki

Toimeksiantaja(t)

Oikeusrekisterikeskus; Mikko Lehtisalo

Tiivistelmä

Viranomaiset ovat aloittaneet digitalisoimaan palveluitaan. Tämä digitalisointi perustuu entisen pääministeri Juha Sipilän hallituksen hallitusohjelman 'Digitalisoidaan julkiset palvelut' -kärkihankkeeseen. Tiedonhallintaan liittyvän lainsäädännön uudistaminen oli myös osa kyseistä hallitusohjelmaa. Nykyinen Laki julkisen hallinnon tiedonhallinnasta tuli voimaan 1. tammikuuta 2020 ja siinä säädetään myös tietoturvallisuudesta. Tämä vaikuttaa julkisiin IT-hankintoihin.

Ensimmäinen kolmesta tavoitteesta oli selvittää Suomen tietoturvallisuutta koskevan lainsäädännön muutoksia ja muutosten vaikutuksia julkisten IT-hankintojen tietoturvallisuusvaatimuksiin. Toisena tavoitteena oli tutkia, pitääkö julkisten IT-hankintojen tietoturvallisuusvaatimuksissa ottaa huomioon enemmän kuin yksi näkökulma ja kolmantena tavoitteena oli selvittää hyvän vaatimuksen sisältö.

Tutkimuksessa huomattiin, että julkisten IT-hankintojen tietoturvallisuusvaatimuksissa on kolmenlaisia vaatimuksia. Ensimmäisenä ovat viranomaisia koskevat vaatimukset, jotka liittyvät hankinnan kohteen määrittämiseen. Toisena ovat tarjouspyynnössä julkaistavat toimittajaan liittyvät vaatimukset, joilla toimittajan tulee ohjata palvelun tuottamista sekä palveluna tuotettavan kohteen tuottamista. Kolmantena tulevat palveluna tuotettavan kohteen yksityiskohtaiset tietoturvallisuusvaatimukset, jotka asetetaan, kun toimittaja on valittu ja palvelun tuottaminen on alkanut.

Julkisten IT-hankintojen tietoturvallisuusvaatimukset tulisi räätälöidä tapauskohtaisesti. Niiden määrittäminen tulisi olla kiinteä osa hankinnan kohteen määrittelyä, koska tietoturvallisuuden ja muiden osa-alueiden välillä on riippuvuuksia.

Avainsanat (asiasanat) julkiset hankinnat, lainsäädäntö, ohjelmistokehitys, tiedonhallinta, tietoturva, tietoturvallisuusvaatimukset, vaatimustenkäsittely, viranomaiset

Contents

Figures

Tables

1 Introduction

1.1 Context and motivation

The development of digital technologies has put the global society in constant change with increasing speed. Companies are digitalising their operations and processes to get economic benefit. At the same time, they are improving services and offerings by developing new digital business models to fulfil market expectations and to deliver more value to customers. (Sathananthan, Hoetker, Gamrad, Katterbach & Myrzik 2017, IV Methodology.) This trend is called Digital Transformation (DT).

Digital transformation and one of its enablers, digitalisation, are associated with numerous challenges as Rautenbach et al. have stated in their study. One of the challenges according to this study is that digital operational environments cause the need for cybersecurity to protect the organisations and their data from cyberattacks. (Rautenbach, de Kock, & Jooste 2019, III. Methodology.)

The Security Committee in Finland raised the national cybersecurity competence as a challenge in Finland's Cyber Security Strategy. This competence is needed both in business life and public administration. One way to ensure and promote the needed cybersecurity skills is to strengthen the cyber and information security as well as ICT training programmes in vocational schools, universities of applied sciences and universities. (Security Committee 2019, 8-9.)

Public administration has also started to digitalise its own operations and services to citizens. Former Prime Minister Juha Sipilä's government (2015-2019) determined digitalisation as one of the main themes in its strategic programme in 2015. There were several key projects under theme, e.g. "Public services will be digitalised" and "Legal provisioning will be improved". (Prime Minister's Office 2015, 18, 27-28.) As a result of this strategic programme, for example Suomi.fi web service was launched in 2017 (Government Strategy Secretariat 2018, 46) and finally the Parliament of Finland approved a government bill of *Act on Information Management in Public Administration* (Parliament of Finland 2019).

1.2 Legal Register Centre

This thesis is assigned by the Legal Register Centre which is a governmental expert agency in Hämeenlinna. The *Act on the Legal Register Centre* was enacted in 2012 and the agency started to operate on its current form on 1 April 2013. This act brought two state agencies together as a one: previous Legal Register Centre and the ICT Service Centre for the Judicial Administration. The current Legal Register Centre has three values, accountability, service-orientation, and fairness, which are followed in everyday operations with all stakeholders by all public officers. (Legal Register Centre 2019.)

The Legal Register Centre operates under Ministry of Justice. One of its main tasks is to maintain and develop information systems of other agencies under Ministry of Justice and Ministry itself. It also enforces fines, forfeitures and receivables, and functions as a controller of some registers of judicial administration. (Act 625/2012, 1 §.)

The Legal Register Centre has three branches: Operational Management Support Services, Information System Services and Public and Government Services. There are around 160 public officers working at the Legal Register Centre. About half of them are working under Information System Services branch. (Legal Register Centre 2019.)

2 Research frame

2.1 Objectives and constraints

In the beginning of 2020, the previous enactment, *Government Decree on Information Security in Central Government (681/2010)*, hereinafter *Information Security Decree*, was repealed, and the new *Act on Information Management in Public Administration (906/2019)*, hereinafter *Information Management Act,* entered into force. The big change for central government is that there are not any provisions on protection levels in any act anymore. Another big change is that this act is now for public administration, not only for central government as the previous enactment.

There are three objectives in this research. The first objective of this research is to study the change in Finnish legislation regarding information security requirements in public IT procurements. The second objective is to study what the different aspects for data security requirements are in public IT procurements or is there only one viewpoint. The third objective is to study what well-formed requirement is. Based on the results template for single information security requirement is created and the concurrent requirements are renewed to correspond the new legislation.

The following questions guide the study to achieve its objectives:

1. How does the *Information Management Act*, change the information security in central government?
    a. Can the previous data security requirements based on the *Information Security Decree* still be used in public IT procurements?
    b. Are there some totally new requirements?
2. What are the aspects and layers of the information security in public IT procurements?
3. What kind of is a good requirement?
    a. What information is needed in it?
    b. How to make requirement understandable?

The subject-matter of IT procurement can vary a lot. For example, it can be off-the-shelf software or customised software. It may also include data centre services or devices. Figure 1 describes possible contents in public IT procurements.

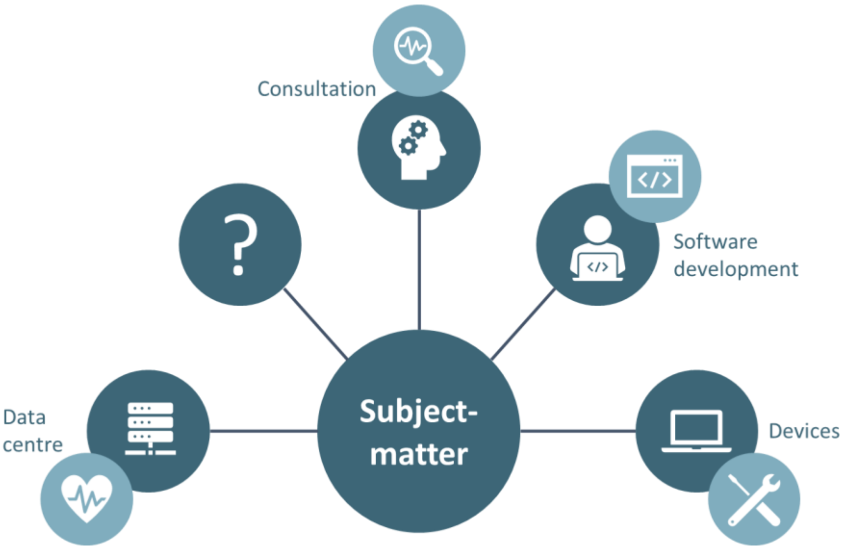


Figure 1. Possible contents in public IT procurements.

Preliminary study showed that most of the public IT procurements in the Legal Register Centre in 2017-2019 have been customised information systems, i.e. software development service, and the protection level in most of them has been PL IV, i.e. basic level. Data centre service has not been part of them.

Preliminary study was executed by defining the time period for two previous years so that the number of procurements were sufficient for analysis. During this time, the concurrent information security requirements were with certainty in use. The data for pre-study was retrieved from agreement database and group workspace for procurements.

Based on all that the delineation of this study is the following:

1. The subject-matter is software development service and the output of that is customised information system. All other possible contents of the subject-matter and any relations to them are excluded.
2. The data security level of the data security requirements is so-called basic level. All data security classification related issues are excluded.
3. The analysis done for the chapter 4 of *Information Management Act* is done from the public IT procurement aspect. The daily compliance aspect is excluded.

2.2 Research data and method

This study is qualitative research. Used method is content analysis which consists of interpretation of the law. The legislation under research will be analysed and applied against the general principles of secure coding and other methods and best practices.

Sources of law are used as research data. Generally, the central source of law is the legislation itself but there are also other sources of law. The documents of legislative drafting process and legal literature are considered such sources too as well as the normal habits and methods in different sectors.

Because this legislation is new there are not many different sources of law available. Therefore, the research data consists mainly of statutory text. At first, the repealed *Information Security Decree*, which is used for creating the baseline. Secondly, the current *Information Management Act* and related government proposal are used for describing the current situation. Also, the security agreement and its appendices used before the following of the current *Information Management Act* is part of the research data.

It needs to be noted that term ‘data security’ is used in chapter 4 and in its subchapters instead of its normal synonym information security. The reason is that term data security is used in the English version of the *Information Management Act*. Because chapter 4 contains citations from the act the compliance with the terminology wanted to be maintained by using the same terminology. Term ‘information security’ is used elsewhere in this document and it means the same as data security.

3 Regulations and requirements

3.1 Public Procurements

Public procurements are procurements of any goods and services as well as building contracts funded with public finance (Pekkala, Pohjonen, Huikko & Ukkola 2019, 19). They are decreed in the act 1397/2016 *Act on Public Contracts and Concessions*, hereinafter the *Procurement Act*. The aim of this act is to optimise the use on public monetary resources. It also furthers making of high-quality, innovative and lasting procurements and safeguards fair competition for providers in government procurements (Act 1397/2016, 2 §).

According to Pekkala et al. (2019,16) the public procurements can be divided in four categories:

1. small-scaled procurements (procurement value below national threshold values),
2. national procurements (procurement value over national threshold values but below EU threshold values)
3. EU procurements (procurement value over EU threshold values) and
4. social and health services and other special service procurements as well as licensing agreements.

The valid threshold values for central government authorities are shown in Table 1 (ibid., 19).

Table 1. National and EU threshold values in public procurements for central government authorities.

Type of Procurement	Threshold Value (VAT excl.)
Goods and services	60 000 € (national), 144 000 € (EU)
Building contracts	150 000 € (national), 5 548 000 € (EU)
Social and health services	400 000 € (national)

The *Procurement Act* does not apply to small-scaled procurements. Instead, general administrative laws are applied to them; the act 621/1999 *Act on the Openness of Government Activities*, hereinafter *Openness Act*, and the act 434/2003 *Administrative Procedure Act*. The *Procurement Act* applies to the three other categories of procurements. (Pekkala et al. 2019, 26.)

The whole procurement process consists of several procedures (Kuuttiniemi & Lehtomäki 2017, 52). However, four main phases presented in Figure 2 can be found there.

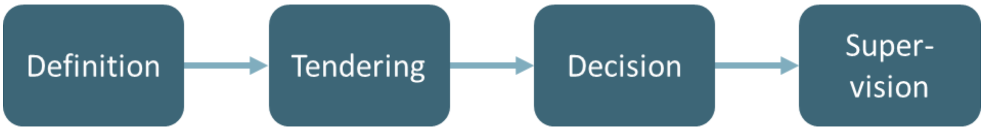


Figure 2. Four main phases of procurement process.

All the main phases and procedures in them are now presented straightforward and simplified with the following constraints. At first, the presumption is that the information system procurements exceed the EU threshold value. Therefore, only those procedures used for procurements exceeding the EU threshold value are introduced here. Secondly, it is assumed that the funding for the procurement is arranged. The last presumption is that the contracting entity follows the non-discriminatory manner and other rules throughout the whole procurement process.

The procurement process is more complicated than the following description shows. There are, for example, standstill periods, time limits and detailed requirements for content of the call for tenders as well as appealing procedures. Because they are not relevant to the understanding of the big picture of the procurement process, they are excluded to keep the description simple.

3.1.1 Definition phase

As Pekkala et al. (2019, 358) state, the preparation task is the most important matter in the public procurement, and it needs time and resources from all stakeholders. The more complex the subject-matter of the procurement is the more time and stakeholder cooperation is needed in this task. It is important to all stakeholders to understand that all the decisions and definitions concerning the subject-matter of the procurement and the conditions for procurement are made during the preparation task, and that all this impacts to the result of the whole procurement. There is documentation which need to be composed during the preparation so that it is ready when contract notice and call for tender are published (Act 1397/2016, 68 §).

After the preparation of the procurement, the contracting entity can screen the market with the preliminary market consultations. It gives the possibility for the contracting entity to consult the market and get the information if there are any solutions available. The contracting entity can change the content and specifications of the subject-matter of the procurement on that basis. The possible tools for preliminary market consultations are request for information and technical dialogue (Kuuttiniemi & Lehtomäki 2017, 136-137.) as well as independent market screening, presentations by suppliers, briefings by the contracting entity and utilising experience of different parties, such as other authorities (Pekkala et al. 2019, 361-363).

The procurements exceeding the EU threshold value have many different procedures to choose from. Each of them has its own specialities. The contracting entity needs to choose the most suitable procedure for the future procurement. (Kuuttiniemi & Lehtomäki 2017, 138.) The Legal Register Centre has mainly used the open procedure, the restricted procedure and negotiated procedure. Therefore, only these three procedures are introduced.

The open procedure is the simplest procedure with only one phase. It starts with the publication of the contract notice and call for tender. All willing suppliers can participate in tendering. (Kuuttiniemi & Lehtomäki 2017, 138-139.)

The restricted procedure has two phases. It also starts with the publication of the contract notice and call for tender. After the publications, all willing suppliers can submit a request to participate in the tendering. Based on the requests, the contracting entity chooses the candidates that are allowed to bid. (ibid., 140.)

These two previously mentioned procedures are the preferred procedures and they have no preconditions to fill. The disadvantage in them is that the contracting entity has no possibilities to negotiate with the suppliers during the procurement procedure. The possibility to negotiate during the procedure is useful in complex procurements, e.g. information systems with customised needs.

The negotiated procedure also has two phases. It starts with the publication of contract notice and preliminary call for tender or project description. After the publication, all the willing suppliers can submit a request to participate in the tendering. Based on the requests, the contracting entity chooses the candidates with whom to negotiate the conditions of contract. (ibid., 141.) It should be taken into account that the contracting entity can negotiate only on those terms that are not announced as the minimum requirements of the procurement. The disadvantage of this procurement procedure is that it might be both time- and money-consuming. (Pekkala et al. 2019, 215.)

It is not allowed to use the negotiated procedure in all procurements. However, it is acceptable for contracting entity to use this procedure, inter alia, in the following situations: (ibid., 216)

- procurements which need customisation to fulfil the needs of the contracting entity,
- procurements which include innovative solutions and designing and
- procurements which after open or restricted procedure did not get tenders which comply with the call for tender or obtained tenders are not acceptable.

After the preparation and possible screening of the market have been conducted and the procurement procedure is selected contracting entity needs to compose and publish the contract notice and the preliminary call for tender. Now the definition phase has been done, and it can be moved to the next phase.

3.1.2 Tendering phase

In tendering phase, the performed operations vary between the procurement procedures. The different tendering phase processes are described for open, restricted and negotiated procedures.

In the open procedure, the tendering phase is the simplest. It includes receiving and opening the tenders, checking the suitability of the tenderers and if the tenders comply with the call for tenders, and finally comparing the tenders. If the tenderer is not suitable or the tender does not comply with the call for tenders, the contracting entity makes the decision on exclusion and notifies it separately or in final decision phase. (Kuuttiniemi & Lehtomäki 2017, 52)

In the restricted procedure, the first task in the tendering phase is receiving the requests to participate in tendering from the willing candidates. The contracting entity needs to evaluate the suitability of the candidates and make the decision who can participate in tendering. If the candidate does not meet the requirements set in the contract notice and call for tenders, the contracting entity composes the decision on exclusion and notifies it. After that the contracting entity composes call for participation in tendering and sends it to the accepted candidates. (Pekkala et al. 2019, 213.)

After that the contracting entity receives and opens the tenders. Then it checks if the tenders comply with the call for tenders. If not, the contracting entity makes the decision on exclusion and notifies it separately or in the final decision phase. (ibid., 213.)

The tendering phase of the negotiated procedure also starts with receiving the requests from the willing candidates to participate in tendering, selecting the participating candidates and possible exclusion of candidates. After that the contracting entity sends the call for participation in tendering and preliminary call for tenders to the candidates. (Pekkala et al. 2019, 217.)

Next, the contracting entity starts to negotiate with the candidates. It is prohibited to negotiate the minimum requirements of the procurement; however, all terms and content of the procurement are negotiable. It is possible to have as many negotiations rounds as possible. When the negotiations are over the contracting entity sends the final call for tenders to the candidates. After that the contracting entity checks if the tenders comply with the final call for tenders. (ibid., 217.)

3.1.3 Decision phase

The decision phase starts with the comparison of the tenders that comply with the call for tenders. The next step is to compose the procurement decision and notify that. This is followed by the signing of the contracting agreement. (Kuuttiniemi & Lehtomäki 2017, 52.) Because of the *Openness Act* the public procurement documents are public. Confidential business or expertise information of candidates can be classified. (Kuuttiniemi & Lehtomäki 2017, 199.)

3.1.4 Supervision phase

The contracting entity needs to supervise the fulfilment of the contracting agreement. If the contracting entity notices any faults or imperfections in delivery, it must inform the supplier immediately and make sure that these defects are corrected. The contracting entity also needs to document the delivery of the service to invoices. (Kuuttiniemi & Lehtomäki 2017, 129.)

3.1.5 Why do public IT procurements fail?

Even though public procurements are well guided by the law, there are several examples of unsuccessful IT-projects and procurements in public administration. For example, the criminal conviction system Ritu exceeded its budget by about 1.6 M€ and was delayed by about 1.5 years (Vänskä 2017). In addition, users found this system difficult to use, and it also slowed down the processes in courts when it was released (Hartig 2014).

The Ministry of Justice ordered an assessment to be made by external consultants to find out what the reasons for the failure of the project were (Hartig 2014). According to the report, several mistakes were made during the whole project. In the beginning the future users did not participate in preparation phase. Also, the steering and the management of the project was inadequate and because of that, the decision making did not work. The supplier had some internal problems with its organisation and communication. After the change of project manager and renewal of project organisation, the quality of the information system improved. (Storås 2014.)

Karoliina Luoto, the procurement consultant said in her interview for Lakimiesuutiset [Lawyer news] magazine that the big problem in public administration's IT-projects is the current operating model. Information systems are renewed every 10-15 years; however, not enough resources are allocated to maintain and further develop them. This leads to the situation that the whole system needs to be renewed at one time which usually takes years. The world usually changes during the long renewal project, and the information system might even be outdated when it is released. One solution to avoid this is to update the old applications constantly. In that way the renewal projects do not become uncontrollable and long-lasting. (Aukia 2018.)

Aapo Koski states in his doctoral thesis that more attention should be paid to public procurements and tendering in the starting phase. The work carried out in this phase has an enormous impact to the following phases and to the whole result. (Koski 2019. 74.)

As a summary, there is not just one cause for failures of public IT procurements. It is a cumulative sum of all the defects within the whole process from the preparation to the development and release.

3.2 Requirements

3.2.1 Requirements engineering

Proper requirements engineering is one of the prerequisites for successful software project. Many experts, such as Leffingwell and Widrig (2003), have found out in their studies that in over 60 % of the cases the reason for failures is the bad requirements engineering. (Haikala & Mikkonen 2011, 61.)

Requirements engineering is the operation in a software project where the requirements of the system are established and maintained (ISO/IEC/IEEE 24765, 2017, 381). Requirements engineering can be divided into two parts: requirements definition and requirements management. (Haikala & Mikkonen 2011, 65). The former is the establishment part and the latter the maintenance part of the requirements engineering.

The requirements definition is a process which consists of requirements elicitation, requirements analysis, requirements specification and requirements validation. The main process in requirements management is the change management of the requirements. The change management process starts with the change request which is then analysed and either approved or rejected. If the change request is approved, then the request in question is updated according to the request. The version control of the requirements is maintained in requirements management as well as the traceability of the requirement. The traceability of the requirement means that the requirement can be traced from its definition to its deployment and testing. (Haikala & Mikkonen 2011, 63-76.)

The earlier explained structure of requirements engineering is showed in Figure 3.

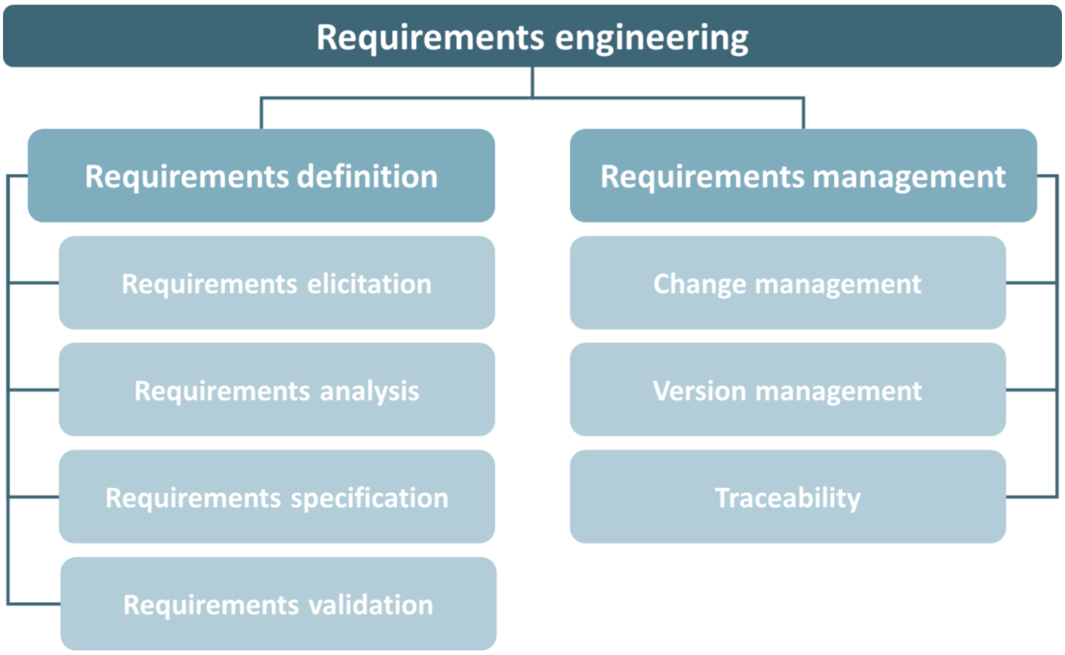


Figure 3. Structure of requirements engineering.

In literature (Haikala & Mikkonen 2011, 61; Robertson & Robertson 2014, 40-42) requirements are typically divided into three categories:

- functional requirements,
- non-functional requirements and
- constraints.

According to Robertson and Robertson (2014), the functionality of the software, in other words, what the information system must do, are specified in functional requirements. These functionalities are necessary for the system to work, and they are used by software developers to develop the software. (253-254.)

Non-functional requirements, on the other hand, describe the quality features of the software. They describe, for example, the usability and security of the system. (ibid., 276-277.) In the other words, non-functional requirements describe the qualities the system must fulfil to operate as it needs to operate.

Constraints are the kind of requirement used to give limitations and restrictions to the system or even the whole project (ibid., 41-42). An example of such constraining requirement can be the programming language that should be used for system development.

3.2.2 Characteristics of well-formed requirements

Well-formed requirements state what is needed, not how. They define performance or capacity of system, not of the user or other operator. Well-formed requirements can contain conditions and be limited by constraints. Conditions are measurable quantitative or qualitative attributes and needed to complete the requirement. Constraints, on the other hand, set restrictions for implementation and can for example be originated from legislation or from existing implementation. (ISO/IEC/IEEE 29148:2018, 10-14.)

When requirements are expressed by using natural language, they should be written with full sentences and with an active voice, i.e. with subject and verb. Sentences shall be completed with constraint of action, object and conditions. It is not mandatory to use all of them in all cases. (ISO/IEC/IEEE 29148:2018, 11.)

According to ISO/IEC/IEEE 29148:2018 standard, it should be agreed on specific keywords that guide if the requirement is mandatory or non-mandatory or shows preferences and goals or suggestions and allowances. In mandatory requirement 'shall' should be used and in non-mandatory 'will'. Preferences and goals should be expressed with 'should' and suggestions and allowances with 'may'. (ISO/IEC/IEEE 29148:2018, 11.) The possibility to use such keywords is fully dependent of characteristics of used language.

Requirements should be written using positive statements but one should avoid using vague and general terms. The use of ambiguous terms requirements become difficult or impossible to verify. Examples of such terms are superlatives, subjective expressions, adverbs and comparative phrases. Expressions like 'if possible' should also be avoided because they set loopholes. (ISO/IEC/IEEE 29148:2018, 14.)

The international standard ISO/IEC/IEEE 29148 (2018, 12-13) also specifies nine characteristics for an individual requirement which every requirement should possess. These characteristics are listed and explained in Table 2.

Table 2. Characteristics of an individual requirement.

Characteristic	Description
Necessary	Every requirement should have a need which cannot be fulfilled with another requirement.
Appropriate	The content of the requirement is relevant and is suited to the level of entity, avoiding any unnecessary constraints and allowing independent implementation of the requirement.
Unambiguous	The individual requirement is easy to understand.
Complete	There is no need for any other information to understand the individual requirement.
Singular	The individual requirement is particular.
Feasible	The implementation of the individual requirement is achievable by resources of the project.
Verifiable	The realisation of the individual requirement can be proven after its implementation.
Correct	The description of the individual requirement is accurate and correctly describes the need.
Conforming	The individual requirement conforms to the form and language requirements set in advance.

3.3 Legislative drafting process of the Act on Information Management in Public Administration (906/2019)

The Finnish legislative drafting process consists of seven stages: preliminary preparation, regulatory drafting, consultation, continued drafting, review by the government, parliamentary review and enactment. There needs to be an initiative for the legislation before the process starts. After the process, the act is published in the Statute Book and the enforcement and the monitoring of the act begins. (Finlex n.d., Legislative Drafting Process Guide.)

The initiative for the *Information Management Act* came from Government Programme of former Prime Minister Juha Sipilä's government. It was essential part of one key project of the programme called *Public services will be digitalised*. The objective was to establish one ordinary law for information management. (Prime Minister's Office 2015, 26-27.)

The preliminary preparation work started in November 2016 when the Ministry of Finance appointed a preparatory body to research the development needs of information management legislation. The term of the preparatory body was 17 November 2016 - 31 May 2017. The first target timetable to enter the new act into force was March 2018. (Ministry of Finance 2016.)

The preparatory body published its report in September 2017. It was stated in the report that concurrent legislation was fragmented, plentiful and inaccurate and did not correspond to operational environment of the 21st century. It was also noticed that information management area contained both common and sector-based regulation which is partly overlapping and parallel. According to the report, the basis of the ordinary law should be clear so that it is possible to cancel and equalise the overlapping and parallel regulation. (Ministry of Finance 2017a.)

The legislative drafting process continued and the aim for government proposal was spring term 2018. The second target to enter the new act into force was in the beginning of 2019. (Ministry of Finance 2017b.)

The regulatory drafting work started in January 2018 when the Ministry of Finance set both a working group and a steering group to support the working group. The term for both groups was 10 January 2018 - 30 September 2018. The working group established a draft government bill (Ministry of Finance 2018a.) and requested comments for the draft in August 2018 (Ministry of Finance 2018b).

The Ministry of Finance prepared the government bill during its term and it was reviewed by the Government in December 2018. The decision of the Government was to submit the government bill to Parliamentary review. (Finnish Government 2018.)

The preliminary debate for the government bill also took place in December 2018. The government bill was then sent to the Administration Committee for its report. The Administrative Committee then asked for a statement from the Constitutional Law Committee which gave its statement in February 2019. The Administration Committee gave its report in March 2019. The bill was then debated in two plenary sessions in March 2019 and the Parliament approved the bill. The parliament gave its response in June 2019 (Parliament of Finland 2019) and the president approved the act in August 2019.

3.4 Digital security in public sector

Digital security is a new and non-stabilised term also used by the Organisation for Economic Co-operation and Development (OECD). Digital security means the issues related to risk management, continuity and contingency, information security, data protection and cybersecurity, as showed in Figure 4. (Ministry of Finance 2020b, 16.)

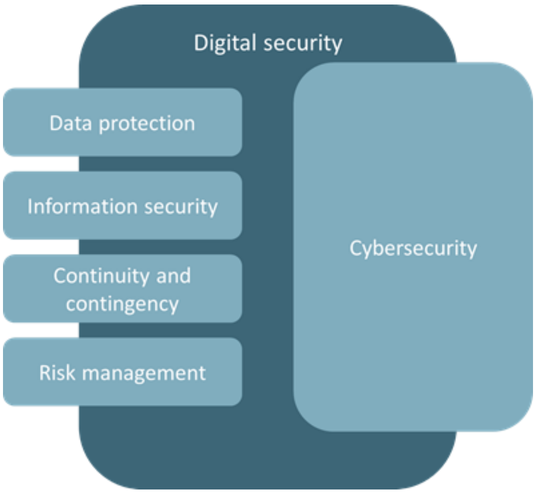


Figure 4. Digital security after the Ministry of Finance.

As showed in Figure 5, the Ministry of Finance is responsible for steering the digital security in public sector. To fulfil this, it set up the Strategic Management Group for Digital Security. The mission of the group is to operate in the strategic level by creating national digital security cooperation model and coordinating its fulfilment. It also evaluates digital security situation in public administration. (Ministry of Finance n.d., Digitaalisen turvallisuuden strateginen johtoryhmä.)

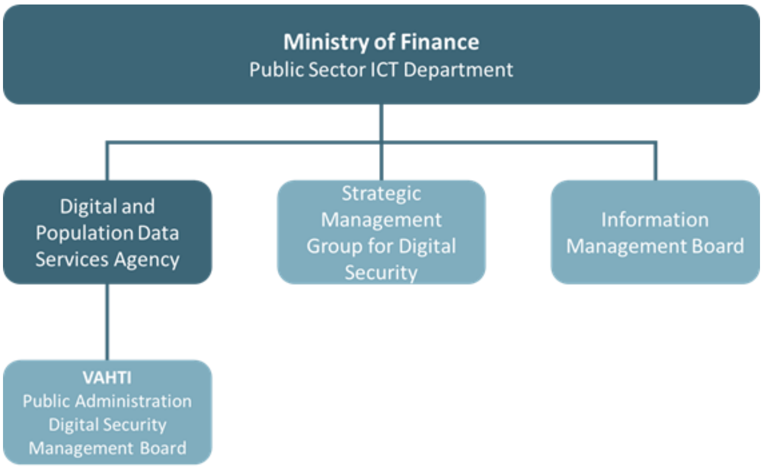

Ministry of Finance
Public Sector ICT Department
Digital and Population Data Services Agency
Strategic Management Group for Digital Security
Information Management Board
VAHTI
Public Administration Digital Security Management Board

Figure 5. The structure of steering and developing digital security in public sector.

The Ministry of Finance has also nominated the Information Management Board. The board is promoting the development and enforcement of the information management in public administration. This can be done, for example, by publishing concrete recommendations. (Ministry of Finance 2020a, Bulletin 27 January 2020). The operation of the board is based on *Information Management Act* (Act 906/2019, 10 §).

The Digital and Population Data Services Agency, hereinafter DVV, operates under the Ministry of Finance. DVV has nominated the Public Administration Digital Security Management Board, VAHTI, which is an operational level and cross-management group. The scope for VAHTI is to improve the digital security, the security culture and attitude in public administration. VAHTI also coordinates the cooperation of the organisations which are responsible for service production. In addition, it produces a situational picture of the digital security in public administration. VAHTI participates in operationally executing the digital security development programmes and projects set by the Ministry of Finance. (DVV n.d., Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI.)

In addition, a Cyber Security Director also operates in Finland. This post is established at Ministry of Transport and Communications and its objective is to coordinate the development of cybersecurity in Finland. (Security Committee 2019.)

4 Results

4.1 Analysing content of subject-matter

Data security requirements define the wanted security level for the subject-matter. To set up a certain security level, the authority needs to define of the content of subject-matter, in other words service.

The service consists of two parts, service production, and service output. The authority needs to understand the big picture of the service. Depending on the content of the subject-matter, there can be, for example, more than one output and this can lead to the situation where service production can include more sections.

In this case, where the subject matter is the development work of a customised information system, there is only one service output, the customised information system. On the other hand, service production can be divided into two sections: the administrative part including management and controlling work and the software development work which can still be separated in two more sections. These are the development part and the maintenance part because nowadays a trend in software development is to use agile methods. The idea of agile methods is to create value to customers as early as possible. Therefore, the information system is developed and released in smaller functional pieces so the software can be in production while it is still developed. The previous waterfall method first developed the software and then released the whole system at one time.

The needed security level of service production fully depends on the required security level of the service output. When the authority is defining the properties and features of the service output, it also needs to define the required security level for it.

The key principles in procurements are equitableness, non-discrimination, and transparency. This means, for example, that brands cannot be used when defining the subject-matter. So, this leads to the situation that detailed requirements cannot be defined to the system. In the case of customised information system, it is not necessarily known what technology the system is based on.

As it can be seen there are relations and dependencies between these actors and the combination seems to be confusing. Therefore, the model of three-level requirement setting for public IT procurements was created to clarify the integrity. This model is showed in Figure 6.

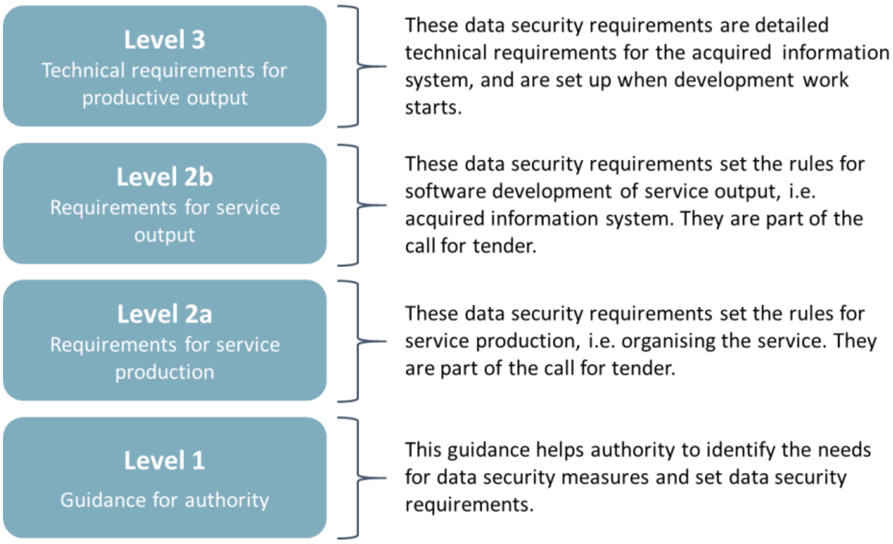

Level 3
Technical requirements for productive output
These data security requirements are detailed technical requirements for the acquired information system, and are set up when development work starts.
Level 2b
Requirements for service output
These data security requirements set the rules for software development of service output, i.e. acquired information system. They are part of the call for tender.
Level 2a
Requirements for service production
These data security requirements set the rules for service production, i.e. organising the service. They are part of the call for tender.
Level 1
Guidance for authority
This guidance helps authority to identify the needs for data security measures and set data security requirements.

Figure 6. The three levels of data security requirements in public IT procurements.

The first level of the data security requirements are the requirements are set by the authority. The purpose of these first level requirements is to ensure the data security requirements are suitable and customised for the subject-matter and cover all parts of the acquired service and its outputs. These are treated in more detail in chapter 4.2 Defining the required security level of the subject-matter.

The second level requirements in Figure 6 have two parts; however, there can be more of them. The amount depends on the amount of service production sections. Here, in this case, there are two as explained earlier. These second level requirements are steering the production of service output so that the output fulfils the required security level. These requirements are part of the call for tender and therefore, it is important that they are set up carefully and customised to suit the subject-matter. The data security requirements from the *Information Management Act* need to be observed in these requirements. This is discussed in more detail in chapter 4.3 Data security in the Information Management Act.

The third level requirements will be set when the tendering is finished, and the supplier has been chosen. Then the implementation method is known, and the detailed technical requirements can be set. These requirements can, for example, be detailed hardening requirements or configuration details. These are set during development project and documented there. Because setting up the third level requirements is not part of any phase of the procurement process and therefore out of the scope of this study, they are not treated more detailed in this document.

4.2 Defining required security level of the subject-matter

Confidentiality, integrity and availability, the CIA-triad, are the elementary principles in data security. The authority shall observe these three factors when eliciting the required security level of the subject-matter and assessing the risks. The authority also needs to observe the requirements from the *Information Management Act*.

Definition work is combination of different factors and issues with many relations and dependencies. All the requirements that are written as a result of identification and analysis of issues may not necessarily be data security requirements but requirements for other area. Figure 7 is clarifying this.

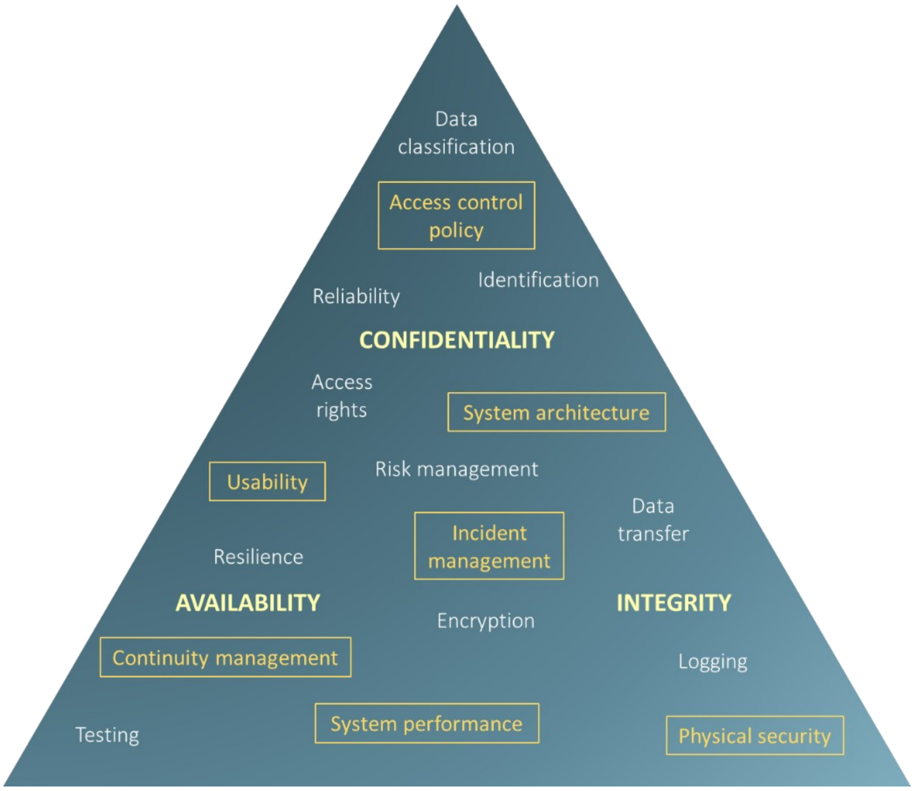


Figure 7. CIA-triad with dependencies from Information Management Act.

The issues applied in the *Information Management Act* are written with white font and lower-case characters. They have impacts on and are impacted by the issues which are elicited when the subject-matter is defined. These issues are written with pale-orange colour and lower-case characters with border lines around them. Both issues have impacts on and are impacted by the principles of data security which are written with upper-case characters and pale-yellow colour.

For example, there might be a certain demand and requirement for system performance. It is not a data security requirement but has impacts to the availability of the system. To give another example, in the *Information Management Act*, there is a requirement for the management of access rights. This protects the confidentiality of the system. This feature needs to be observed in the system architecture.

The issues presented in Figure 7 do not present a complete list of all possible issues but rather demonstrate possible issues. The definition of data security requirements is easier when the persons behind the definition work understand this big picture and perceive the dependencies.

When defining the security level of the customised information system, the authority needs to define at least the following issues:

- the criticality of the information system,
- the content and classification of the data,
- geographical location for data storage and
- data flows and integrations.

The authority also needs to define the following issues related to the service production:

- needed competence and competence level for supplier's employees, data security included,
- geographical location for service production and
- the classification of data given to the supplier or where the supplier has access.

There is a list of supporting questions in Appendix 1. They can be used for eliciting the information security related needs which are then analysed and written as data security requirements. There are questions concerning the data, supplier and information system.

4.3 Data security in the Information Management Act

This chapter introduces the data security part of the *Information Management Act*. There are six sub-chapters, one for each section which issues provisions on non-security-classified issues on chapter 4 Data security of the Information Management Act. The last section which issues provisions on security classified documents is excluded because security classified documents are not part of this study.

Each subchapter treats its own section of the act. Every section has been analysed from customised information system aspect by asking the following questions:

- Does this section have any impacts on service production?
- Does this section have any impacts on service output?

The analysis presented in this chapter includes the minimum content. The final content of data security requirements is dependent on the definition of subject-matter and risk assessment related to that. The detailed requirements are not included; instead, the themes to consider are.

4.3.1 Identification of tasks requiring reliability and ensuring reliability (12 §)

The following is issued in this section:

> *An information management entity shall identify the tasks whose performance requires special reliability from persons employed by it or acting on its behalf. The preconditions for carrying out a security clearance of a person are provided in the Security Clearance Act (726/2014). The right of an employer to acquire personal credit data on an employee in order to establish his or her reliability and to process data on drug use testing are governed by the provisions of the Act on the Protection of Privacy in Working Life (759/2004).* (Act 906/2019 English version, 12 §.)

To fulfil this section the authority shall identify the tasks the supplier needs to perform to produce the service and then analyse if they require or enable access to the authority's confidential data. After that the authority needs to analyse if there is a need for ensuring the reliability of the supplier's employees by performing security clearances of the person or by other possible means.

Using the security clearances of the person for the supplier's employees need to be set as a data security requirement. An additional requirement of keeping a book of all the employees who have been cleared can also be set.

4.3.2 Data security of datasets and information systems (13 §)

This section is the largest unity. It includes issues from different areas and has dependencies between them and data security. This was presented in Figure 7 in chapter 4.2 Defining the required security level of the subject-matter.

According to government proposal (HE 284/2018, YKSITYISKOHTAISET PERUSTELUT 13 § [HE 284/2018, DETAILED ARGUMENTS 13 §]), this first subsection is about risk management. The essential risks for both datasets and information systems shall be identified and analysed. On that basis, data security controls which need to be implemented are determined.

> *An information management entity shall monitor the state of the data security of its operating environment and ensure the data security of its datasets and information systems over their entire lifecycle. The information management entity shall determine*

> *the material risks to data processing and dimension the data security measures in accordance with the risk assessment.* (Act 906/2019 English version, 13.1 §.)

Because the supplier is developing and perhaps maintaining the information system, there should be requirement for the supplier to perform risk assessment for service production. There should also be a requirement for regular threat modelling of the information system. The best results would be achieved if this were done in cooperation. The acquirer has the best knowledge about the operating environment and the substance and the supplier about the technical implementation.

The following is provided in the second subsection:

> *The resilience and operational availability of the information systems that are material with regard to performance of the tasks of the authorities shall be ensured with adequate testing on a regular basis.* (Act 906/2019 English version, 13.2 §.)

There are two issues included in this subsection. The first is about resilience and the second is about operational availability of the information system. According to the act, the only control to ensure these is regular testing.

It is written in the government proposal (HE 284/2018, YKSITYISKOHTAISET PERUSTELUT 13 § [HE 284/2018, DETAILED ARGUMENTS 13 §]) that resilience shall be tested to verify the operational continuity and keep data security measures up to date. There should be a requirement for the supplier to have and maintain a documented continuity plan for service production which is known by the employees and tested. This should cover the whole service production and all processes.

The resilience of the system needs more than regular testing. Therefore, there should be a requirement for the supplier to use general secure design and programming principles in software development of the information system. There can, for example, be requirement to follow OWASP Top 10 which includes both parts.

To ensure the quality and adequacy of data security testing, it would be beneficial to require both manual and automated data security testing. Manual testing verifies for example the functionality of data security features and correctness of configurations and hardening controls. Automated test, again, can include a code analysis and vulnerability scanning and can be part of DevOps operations. When testing the resilience of the system, performance testing should also be executed. Normally this is not part of the data security testing, so the requirement is not usually included in data security requirements.

In addition, to ensure the operational continuity of the system, there should be requirements for operations related to continuity. For example, there can be requirement for the supplier to participate in the writing of recovery plan and maintaining the documentation of installation, updating, recovering and removing of the system.

Another issue of this subsection, operational availability, includes the requirement for verifying that the information system is easy to learn, its logic is easy to remember, and it supports user's work tasks (HE 284/2018, YKSITYISKOHTAISET PERUSTELUT 13 § [HE 284/2018, DETAILED ARGUMENTS 13 §]). This is an excellent example of an issue affecting data security; however, it is not part of data security itself. This issue belongs to usability area. When the system is easy to use it reduces the possibility for using the system incorrectly and in that way improves the data security. These requirements belong to usability area and need to be included in the requirements specification.

The content of the third subsection of section 13 also belongs under other area than pure data security even though it affects it.

> *The authority shall plan the information systems, the internal structure of the information pools and related processing so that the publicity of documents can be easily implemented.* (Act 906/2019 English version, 13.3 §.)

The authority shall plan its information systems and the data structures of information pools so that the structure supports setting the data and documents easily to be either public or confidential. There can be general data security requirement that the system needs to support the processing and storage of both public and confidential data.

The fourth subsection provides the data security in acquisitions. It can be said that this whole study is researching this area.

> *In its acquisitions, the authority shall ensure that appropriate data security measures have been implemented in the information system to be acquired.* (Act 906/2019 English version, 13.4 §.)

When starting the acquisition, it is important that the authority carefully defines the subject-matter, i.e. service, assesses the risks and defines the data security requirements based on the both actions. As important is that the authority inspects and monitors the service regularly.

The authority can also order the third party to make the security assessment. Sometimes there can even be requirement from legislation that the information system needs to be audited and approved before it can be taken into production use. The fifth subsection itself does not lay down provisions on auditing the system but refers to other legislation.

> *Separate provisions are laid down on the assessment of the data security of the information systems and telecommunications arrangements of the authorities.* (Act 906/2019 English version, 13.5 §.)

The authority needs to recognise the possible need for data security assessment when it prepares the acquisition and makes a requirement which enables to perform assessment by the authority itself or by the third party. The target of the assessment can for example be the service production processes, the service output, both or certain smaller part.

4.3.3 Transfer of data in a data network (14 §)

Section 14 lays down the provisions on data transfer through public data network. The following is provided in the first subsection.

> *An authority shall perform the transfer of data in a public data network using an encrypted data transfer connection or practice if the transferred data are secret. In addition, the data transfer shall be arranged so that the recipient is ascertained or identified in a sufficiently data secure manner before the recipient is allowed to process the transferred secret data.* (Act 906/2019 English version, 14.1 §.)

When the authority starts the cooperation with the supplier, the authority should give instructions how the supplier should handle the confidential data of the authority. There should also be a requirement to the supplier for handling the confidential data of the authority and another requirement for informing its employees about the instructions and practices set by the authority.

There can also be a requirement for the use of separate safety premises. This depends on tasks performed by the supplier’s employees and the confidentiality of data. The requirement usually includes at least the technical requirements for network connections, workstations, and physical security of safety premises. The reason for requiring safety premises can be maintenance tasks for production environment containing personal data.

There should be a requirement for encrypted data transfer in data security requirements of the system. This should cover at least the system interfaces which send or receive data through public data network.

The needed cryptography algorithms depend on data confidentiality. Finnish National Cyber Security Centre is maintaining a guideline on cryptographic requirements for confidentiality, which can be used for finding the suitable level. This can be set already in the data security requirements which are published in the call for tender or when the software development starts.

If needed, the encryption can also be required in an internal data network. In such cases it needs to be observed that encryption and decryption may cause latency and demand processing time and capacity from the processors. The more secure algorithm is used, the more power it requires for encryption and decryption.

The second subsection is about data transfer where the recipient is general public.

> *Identification of the user in digital services provided to the public is governed by the Act on the Provision of Digital Services (306/2019).* (Act 906/2019 English version, 14.2 §.)

When the authority is defining the subject-matter, i.e. acquired information system, the authority needs to elicit if the system provides digital services for the public. In such case there will become data security requirements from the sections 5 and 6 of the *Digital Service Act*.

4.3.4 Ensuring dataset security (15 §)

This section sets provisions on ensuring dataset security and has two subsections. The first subsection includes a list of data security measures which the authority needs to follow. They are set in six paragraphs. These issues are mostly targeted at the authority’s operations; however, some issues may cause data security requirements for service production or service output.

> (Act 906/2019 English version, 15.1 §): *An authority shall ensure, with the necessary data security measures, that:*
>
> *1) the unaltered state of its datasets has been sufficiently ensured;*
>
> *2) its datasets have been protected against technical and physical damage;*
>
> *3) the authenticity, timeliness and accuracy of its datasets have been ensured;*
>
> *4) the availability and usability of its datasets have been ensured;*
>
> *5) the availability of its datasets is restricted only if access to the information or processing rights have been separately restricted in the law;*
>
> *6) its datasets can be archived, as required.*

The unaltered state of datasets, issued in paragraph 1, can be partly ensured with logging which is treated later in this document in chapter 4.3.6 Compilation of log data (17 §). the measures related to identity and access management also give some controls for this paragraph. Identity and access management is treated in chapter 4.3.5 Management of access rights to information systems (16 §).

If subject-matter has data centre included, then the second paragraph will set clear data security requirements. In this case some of the requirements related to continuity issues may concern this indirectly, which were already treated in chapter 4.3.2 Data security of datasets and information systems (13 §).

Because of the digitalisation, the issues in paragraph 4 are essential. The authorities are also handling more and more the information with the information systems and depend on their information pools where the needed information is. Ensuring availability, the data security requirements are related to continuity issues. The usability in this paragraph means that the data is in usable form (HE 284/2018, YKSITYISKOHTAISET PERUSTELUT 15 § [HE 284/2018, DETAILED ARGUMENTS 15 §]). Ensuring this there can be requirement concerning the transferability of data from the system to another. With this requirement it can be made sure that if there is need for change the information system, the data can be migrated and used in the new system.

The fifth paragraph sets requirements for restricting the access to data. In practice this is carried out with access rights. This issue is treated later in this document in the next chapter 4.3.5 Management of access rights to information systems (16 §).

The last, the sixth paragraph of the first subsection lays down provisions on archiving the data. The principles for setting up the data security requirements for archiving and retaining archived data are the same as the data handled and stored in the information system. The new life cycle for the data is beginning, and the same recognition and risk assessment procedures need to be executed and corresponding data security requirements set.

There is also other legislation which issues provisions on archiving. The most essential are the General Data Protection Regulation, i.e. *GDPR* ((EU) 2016/679), *Data Protection Act* (1050/2018) and *Archiving Act* (831/1994). The first two apply when the archived data includes personal data.

The second subsection is about the physical security of the premises.

> *The datasets shall be processed and stored in premises which are sufficiently secure with a view to implementing the requirements relating to the reliability, integrity and availability of datasets.* (Act 906/2019 English version, 15.2 §.)

Depending on data and its confidentiality, there can be general data security requirements for the supplier’s premises. They can include demands on secure areas or separate safety premises. The authority can also set requirements for the geographical location of service production. This should also include the location requirement of supplier’s supporting information systems used for service production and storing customer data and customer’s data.

4.3.5 Management of access rights to information systems (16 §)

If the data is not public, it should not be available for all. Section 16 lays down provisions on access rights to information systems and the management of them.

> *The authority in charge of the information system shall determine the access rights to the information system. The access rights shall be determined in accordance with the needs relating to the tasks of the user and they shall be kept up-to-date.* (Act 906/2019 English version, 16 §.)

Because the authority needs to be aware of all the persons who has access to its confidential data, there should be a data security requirement for the supplier to keep the books of all its employees who participate in the acquired service production and have access to confidential data of the authority. Another requirement should be set for the supplier to restrict the access to data from other employees who are not participating in the service production of the acquired service production. All the participating employees must have personal user IDs for accessing the tools and data to execute service production duties. There needs to be a requirement for documented process of access rights management, and all the access rights related to service production is to be documented.

The authority also needs to plan and define the different user roles for the acquired system and how the identity and access management is implemented into system. These requirements are not usually data security requirements. Their implementation may need data security measures.

4.3.6 Compilation of log data (17 §)

Compilation of log data obligates the authority to gather log data from the use of information systems.

> *An authority shall ensure that the necessary log data is compiled of the use of its information systems and the disclosure of information therefrom if the use of the information system requires identification or other login. The purpose of use of log data is to monitor the use of the information in the information systems and its disclosure and to investigate technical errors in the information system.* (Act 906/2019 English version, 17 §.)

Every log must have demand. The best benefit from logs is achieved when the content of the log, based on the demand, is planned. This means that not all the information the system is producing is collected but the information is parsed and only the essential data is compiled to the log.

This requires identification of logging points, i.e. defining the information on what needs to be logged, and planning the structure of logs. One example of log structure is key-value-structure, where the key provides the logging point and value is system log data from that point. When the content and structure are defined carefully, which makes finding the needed information from logs is easier.

The storage period of log is based on demand of use and need to be defined separately to every log. Therefore, the storage period can vary between different logs.

The logs are needed to find out causes for technical problems or person who processed certain data at certain time period, i.e. audit trail. As can be seen, the latter includes personal data. Therefore, technical logs and audit trails need to be separated from each other.

An audit trail is important because it gives legal protection to both public servant who has processed the data as part of his or her duty, and the citizen whose data has been processed. It needs to be noted, that *GDPR* and *Data Protection Act* lay down provisions on audit trail.

According to normal judicial practice, log data is confidential under the *Openness Act* 24.1p7 §. Therefore, access to logs, both technical and audit trail, needs to be restricted. The management of access right need to be planned, and access to logs must be based on work tasks.

To ensure the unaltered state of logs, it is a good solution is to send the logs in real-time to centralised logging system, which is designed and implemented to store the logs safely. This also lowers the risk of losing the logs for example during major incident of the information system which requires restoring the whole system.

According to government proposal (HE 284/2018, YKSITYISKOHTAISET PERUSTELUT 17 § [HE 284/2018, DETAILED ARGUMENTS 17 §]) the authority must be able to solve the disclosure of information from system and legitimate grounds for that from the logs. The authority must also log actions which are directed to data, such as saving, changing, deleting and viewing.

To fulfil this section the authority should include a data security requirement for implementing logs to acquired information system. If the authority has centralised logging system, there can be a requirement to send system logs there. It would be also good to have requirement for the supplier to take part in log planning and writing together with the authority and maintain documentation on implemented logging. The supplier should also be required to log its own service production systems.

4.3.7 The removal of protection levels

Before the current *Information Management Act* the it was possible to classify the confidential data with protection level, PL. Protection level classification was used to protect personal data and it had four levels. *Information Security Decree* sets direct requirements how to protect data on which protection level. Now that protection levels are removed, also the related requirements are removed, which can cause confusion.

It needs to be remembered that even though the protection levels are removed from the legislation, the basis for data protection is not removed, and the principles are the same. The data must still be protected as before.

When the authority is defining the subject-matter, it analyses the need for data protection in the same way that it previously analysed the need for classification of the data with protection levels. Now the measures are not derived from legislation according to protection level but the authority itself sets the needed measures to fulfil the authority’s own data security standard. The authority can still use the same measures but needs to avoid using term protection level anymore.

4.4 Information Management Act vs. Information Security Decree

One part of the study was to compare the current *Information Management Act* with repealed *Information Security Decree*. The aim for that was to solve if the content of data security requirements in use was still usable in case of correspondences.

The comparison was made by comparing the current act against the repealed decree. Even the partial correspondences were accepted and listed. The results are presented in Table 3 below.

Here is guidance of the used reference methods in the Table 3. The marking § 12 refers to the whole section. The marking § 13.1 refers to the first subsection of section 13 whereas § 13.2 to the second subsection of the same section. Marking § 5.1p1 refers to the first paragraph under the first subsection of section 5 whereas § 5.1p2 refers to the second paragraph under the first subsection of section 5.

The content of the sections, subsections, and paragraphs in Table 3 is from the English translations of the *Information Management Act* and the *Information Security Decree*. They can be found in Finlex service. However, the comparison work was carried out with Finnish versions.

Table 3. Comparison between the *Information Management Act* and the *Information Security Decree*.

Information Management Act	Information Security Decree
§ 12 *An information management entity shall identify the tasks whose performance requires special reliability from persons employed by it or acting on its behalf. The preconditions for carrying out a security clearance of a person are provided in the Security Clearance Act (726/2014). The right of an employer to acquire personal credit data on an employee in order to establish his or her reliability and to process data on drug use testing are governed by the provisions of the Act on the Protection of Privacy in Working Life (759/2004).* (Act 906/2019 English version, 12 §.)	**§ 5.1** *In order to implement information security, a central government authority shall ensure that* **p3** *the duties and responsibilities related to the handling of documents are defined;* **p8** *the reliability of personnel and other persons performing tasks related to the handling of documents is ensured, if necessary, by means of a security clearance procedure and other means available by virtue of law;* (Decree 681/2010 English version, 5 §.)

§ 13.1 *An information management entity shall monitor the state of the data security of its operating environment and ensure the data security of its datasets and information systems over their entire lifecycle. The information management entity shall determine the material risks to data processing and dimension the data security measures in accordance with the risk assessment.* (Act 906/2019 English version, 13 §.)	**§ 5.1** *In order to implement information security, a central government authority shall ensure that* **p1** *any information security risks connected with the activities of the central government authority are identified;* (Decree 681/2010 English version, 5 §.) **§ 6** *Information security measures shall be planned and implemented so that they cover all stages of handling a document, ranging from the preparation or reception of the document to the filing or destruction thereof, including the provision and transfer of the document and the supervision of the handling. In the planning, compliance with data processing obligations shall be ensured also when data processing tasks are carried out on commission of central government authorities.* (Decree 681/2010 English version, 6 §.)
§ 13.2 *The resilience and operational availability of the information systems that are material with regard to performance of the tasks of the authorities shall be ensured with adequate testing on a regular basis* (Act 906/2019 English version, 13 §.)	
§ 13.3 *The authority shall plan the information systems, the internal structure of the information pools and related processing so that the publicity of documents can be easily implemented.* (Act 906/2019 English version, 13 §.)	**§ 4** *A central government authority shall ensure that its planning of information security pursuant to good practice on information management is based on inquiries and assessments conducted by it regarding documents in its possession and the significance of their contents, that the planning is conducted with account of the requirement to ensure good publicity and secrecy structures in information systems, and that the information security measures are geared with consideration of the significance and purpose of use of the information to be protected, of the threats against the documents and the information systems, and of the costs for the information security measures.* (Decree 681/2010 English version, 4 §.)

§ 13.4 *In its acquisitions, the authority shall ensure that appropriate data security measures have been implemented in the information system to be acquired.* (Act 906/2019 English version, 13 §.)	**§ 4** *A central government authority shall ensure that its planning of information security pursuant to good practice on information management is based on inquiries and assessments conducted by it regarding documents in its possession and the significance of their contents, that the planning is conducted with account of the requirement to ensure good publicity and secrecy structures in information systems, and that the information security measures are geared with consideration of the significance and purpose of use of the information to be protected, of the threats against the documents and the information systems, and of the costs for the information security measures.* (Decree 681/2010 English version, 4 §.)
§ 13.5 *Separate provisions are laid down on the assessment of the data security of the information systems and telecommunications arrangements of the authorities* (Act 906/2019 English version, 13 §.)	
§ 14.1 *An authority shall perform the transfer of data in a public data network using an encrypted data transfer connection or practice if the transferred data are secret. In addition, the data transfer shall be arranged so that the recipient is ascertained or identified in a sufficiently data secure manner before the recipient is allowed to process the transferred secret data.* (Act 906/2019 English version, 14 §.)	
§ 14.2 *Identification of the user in digital services provided to the public is governed by the Act on the* *Provision of Digital Services (306/2019).* (Act 906/2019 English version, 14 §.)	
§ 15.1 *An authority shall ensure, with the necessary data security measures, that:* (Act 906/2019 English version, 15 §.)	

§ 15.1p1 *the unaltered state of its datasets has been sufficiently ensured;* (Act 906/2019 English version, 15 §.)	**§ 5.1** *In order to implement information security, a central government authority shall ensure that* **p6** *unauthorised modification and other unauthorised or inappropriate processing of information is prevented by access rights management, access monitoring, and appropriate and sufficient security arrangements concerning information networks, information systems and information services;* (Decree 681/2010 English version, 5 §.)
§ 15.1p2 *its datasets have been protected against technical and physical damage;* (Act 906/2019 English version, 15 §.)	
§ 15.1p3 *the authenticity, timeliness and accuracy of its datasets have been ensured;* (Act 906/2019 English version, 15 §.)	
§ 15.1p4 *the availability and usability of its datasets have been ensured;* (Act 906/2019 English version, 15 §.)	**§ 5.1** *In order to implement information security, a central government authority shall ensure that* **p4** *access to and availability of information in different situations are safeguarded,* […]; (Decree 681/2010 English version, 5 §.)
§ 15.1p5 *the availability of its datasets is restricted only if access to the information or processing rights have been separately restricted in the law;* (Act 906/2019 English version, 15 §.)	**§ 5.1** *In order to implement information security, a central government authority shall ensure that* **p5** *the secrecy and other protection of documents and the information contained therein are safeguarded by granting access to documents only to those who need secret information or personal data recorded in a personal data file for performing their work duties;* (Decree 681/2010 English version, 5 §.)
§ 15.1p6 *its datasets can be archived, as required.* (Act 906/2019 English version, 15 §.)	**§ 6** *Information security measures shall be planned and implemented so that they cover all stages of handling a document, ranging from the preparation or reception of the document to the filing* […]. (Decree 681/2010 English version, 6 §.)

§ 15.2 *The datasets shall be processed and stored in premises which are sufficiently secure with a view to implementing the requirements relating to the reliability, integrity and availability of datasets.* (Act 906/2019 English version, 15 §.)	**§ 5.1** *In order to implement information security, a central government authority shall ensure that* **p7** *the premises for data processing and storage of documents are sufficiently monitored and protected;* (Decree 681/2010 English version, 5 §.)
§ 16 *The authority in charge of the information system shall determine the access rights to the information system. The access rights shall be determined in accordance with the needs relating to the tasks of the user and they shall be kept up-to-date* (Act 906/2019 English version, 16 §.)	**§ 5.1** *In order to implement information security, a central government authority shall ensure that* **p3** *the duties and responsibilities related to the handling of documents are defined;* **p5** *the secrecy and other protection of documents and the information contained therein are safeguarded by granting access to documents only to those who need secret information or personal data recorded in a personal data file for performing their work duties;* (Decree 681/2010 English version, 5 §.)
§ 17 *An authority shall ensure that the necessary log data is compiled of the use of its information systems and the disclosure of information therefrom if the use of the information system requires identification or other login. The purpose of use of log data is to monitor the use of the information in the information systems and its disclosure and to investigate technical errors in the information system.* (Act 906/2019 English version, 17 §.)	In **§ 5.1p6** of the decree it is mentioned *access monitoring*. Otherwise the paragraph in question does not comply with the § 17 of the act. (Decree 681/2010 English version, 5 §.)

This comparison work showed that the current act has largely the same content as the repealed decree. There are also some issues which are laid down only in the current act. As a result of this comparison, it could be said some decree-based requirements can be used and modified with the current act if they otherwise fulfil the criteria of unambiguous requirements. This requires grouping according to the current act and deeper analysis.

4.5 Renewal of requirements

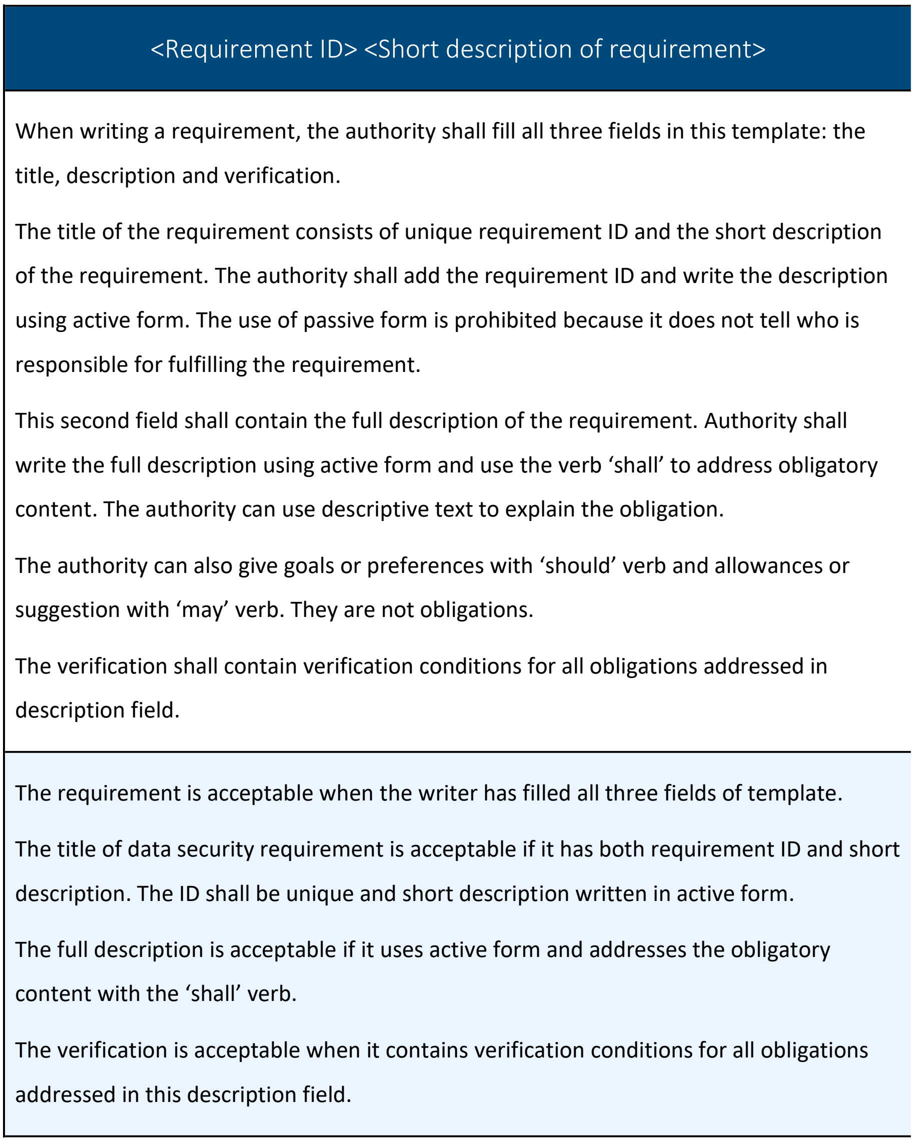
The last issue of this study was to design a template for single data security requirement based on the research results. Then, by using the template and concurrent requirements, new data security requirements are to be written which also fulfils the obligations of the current legislation.

4.5.1 Template for single requirement

The criteria for the template were derived from the principles of good requirement presented in chapter 3.2 Requirements engineering and the operation model in the Legal Register Centre. The Legal Register Centre uses so called minimum requirement set which is maintained by the information security team. The content is based on legislation, the template does not need information about author or rationale. The version of the requirements is the version of requirements document. Therefore, a single requirement does not need version information.

Because the data security requirements are part of the call for tender, they should be consistent and unambiguous. Even though the supplier has the possibility to ask questions during the procurement process, the template should support the linguistic quality and writing measurable requirements.

The template is presented in Figure 8. The template includes guidance written following the same method than is required for writing the single requirement.



<Requirement ID> <Short description of requirement>

When writing a requirement, the authority shall fill all three fields in this template: the title, description and verification.

The title of the requirement consists of unique requirement ID and the short description of the requirement. The authority shall add the requirement ID and write the description using active form. The use of passive form is prohibited because it does not tell who is responsible for fulfilling the requirement.

This second field shall contain the full description of the requirement. Authority shall write the full description using active form and use the verb ‘shall’ to address obligatory content. The authority can use descriptive text to explain the obligation.

The authority can also give goals or preferences with ‘should’ verb and allowances or suggestion with ‘may’ verb. They are not obligations.

The verification shall contain verification conditions for all obligations addressed in description field.

The requirement is acceptable when the writer has filled all three fields of template.

The title of data security requirement is acceptable if it has both requirement ID and short description. The ID shall be unique and short description written in active form.

The full description is acceptable if it uses active form and addresses the obligatory content with the ‘shall’ verb.

The verification is acceptable when it contains verification conditions for all obligations addressed in this description field.

Figure 8. Requirement template with descriptions.

The template consists of three mandatory fields: title, description and verification and all of them need to be filled. The requirement shall be written in active form and obligations addressed by using the verb ‘shall’. The use of immeasurable words, e.g. ‘sufficient’, ‘appropriate’, ‘essential’ and ‘necessary’, shall be avoided. All obligations shall have own verification conditions.

4.5.2 Renewal work

In the Legal Register Centre the data security requirements are in the appendix of a secure agreement. The purpose of the secure agreement is to agree on safety arrangements, confidentiality, data protection and data security. This model remained in new model.

The Secure agreement includes contractual security issues in following areas: sub-contracting, confidentiality and obligation of secrecy, data protection, administrative and physical security, administration of information systems, software security, continuity, security clearances, auditing, and reporting and communication. Concurrent requirements and security agreement included a large number of overlapping requirements, especially in confidentiality and administrative security areas. Many of the overlapping requirements were more contractual issues in nature than pure requirements. Therefore, they were removed from requirements and left as part of the agreement.

The requirements in technical and software development areas were list of singular requirements and did not have cohesion. In other words, they did not guide the supplier to implement built-in security but rather add-on security. The software development was not seen as a combination of design, development, testing, deployment and maintenance.

The renewal work lowered the number from over 100 requirements to less than 15 requirements. The reason for this was the removal of overlapping contractual issues. The other reason for decrease was grouping. Previously, there was a bunch of single requirements with same or nearly same goal. These requirements were grouped and joined.

New data security requirements have data security requirements for general service production work which are related to administrative security. The other part covers the information system and software development. The most significant change in this part was the change from add-on security thinking to built-in security thinking. This change added the requirements to follow OWASP Top 10 and OWASP API Security Top 10 principles and perform both manual and automated data security testing based on OWASP Application Security Verification Standard. They can be followed because the user interfaces of information systems are mostly browser based.

5 Conclusions

This thesis studied how the change in legislation laying the provisions in information security and imposing obligations for public administration, affected information security requirements in public IT procurements. The work was assigned by the Legal Register Centre in Hämeenlinna which organises the development and maintenance of information systems under the Ministry of Justice and arranges public IT procurements.

The results showed that the issues in legislation have remained quite similar. This new act has only a few completely new issues in it compared to the content of repealed decree. The biggest change is in the way of defining the security level for the subject-matter of acquired IT service. Previously, the authorities had the possibility to classify the data to certain protection level and then define the requirements from the decree.

Now when the protection levels are removed, the authorities must define the level and related requirements by themselves according to current legislation and by using risk-based method. Even though the current method might seem totally new, it is based on the same principles as the previous method: the data needs to be protected according to its content, and the protective measures are selected based on that. It seems that the new method is more flexible, and the authorities can apply it more freely to meet their own needs.

The results of the study also showed how important it is to understand the structure of subject-matter when setting up the information security requirements. The subject-matter can be seen as a service which consists of service production and service product issues. The service product in this study, the customised information system, must meet the obligations issued in legislations. This leads to the situation that the service production, software development work and related management and control work, must meet the same obligations too. The nature of these two issues is different so the aspect of information security requirements is also different.

Because the requirements are published as a part of the call for tender, this must be taken into account when defining the subject-matter.

Another aspect of the thesis was to study characteristics of good requirement. Based on past procurements it seemed that some requirements were ambiguous, the number of requirements was high, and requirements did not fit to subject-matter.

The results showed that information security requirements should be measurable and linguistically clear. Because the requirements are part of call for tender, the suppliers make the decision to tender based on them. If suppliers do not understand the obligations, it is a high risk for them to tender. If an acquirer does not understand obligations, how can it monitor fulfilment? Clear and consistent information security requirements help both parties to understand the obligations.

The content of requirements specification needs to be customised case by case even it is possible to have ready sets of requirements. To do that, the content of subject-matter needs to be fully understood. As it can be seen, the themes in this thesis correlate with each other.

6 Discussion

The need for this thesis came from a change in legislation. The effects on IT procurements were not known and they needed to be evaluated. Because the Legal Register Centre has continually ongoing IT procurements, the impacts needed to be known as soon as possible.

The schedule of this thesis was moved forward because the legislative drafting process was constantly delayed. The first target to enter the new act into force was March 2018. Finally, this was on 1 January 2020. The enactment of the act was done in August 2019; hence, the study could be started after that.

The subject for the thesis was information security requirements of the IT procurements. As it is known the concept of IT is wide. Therefore, this study started with pre-study. The purpose for that pre-study was to find what kind of IT procurements were the majority group in the last two years, how was the subject-matter and what tendering procedures were used in the procurements. The study helped to find the most important target group from the IT procurement point of view and set constraints to the thesis.

The results of the pre-study showed that most subject-matters were customised information systems at basic level and did not include data centre services. The trend in tendering procedures was the use of negotiated procedure.

The pre-study also showed that many suppliers had asked questions concerning the content and suitability of concurrent information security requirements. This observation led to include the structure and language of requirements as a part of the thesis as well.

The actual study started by gathering the information about public procurements and tendering procedures. This strengthened the assumption about the importance of content in requirements. Public procurements are strictly regulated; changing the content of procurement is not possible, even though the negotiated procedure allows some adjustment up to a certain point of procedure.

Next the structure of subject-matter was studied. As the pre-study showed, there had been comments and questions concerning the suitability of information security requirements compared to the content of subject-matter. An analysis of concurrent requirements showed that requirements were general, rather “one size fits all” than customised to a certain procurement.

One of the pain points were the responsibilities. It was possible to interpret some requirements so that they were not obligatory. Even though the compliance with key principles of procurement process, i.e. equitableness, non-discrimination, and transparency, restricts to definition of subject-matter, it still should be possible to define what services and with what kind of responsibilities it will be acquired.

Dividing the acquired service into two categories, service production and service output, helped in the next phase, the actual interpretation of law. The act has been written to support authorities to accomplish their duties. In other words, the connection between the act and acquired service is not clear. The act also treats the big picture of information security, and therefore it has dependencies to other areas than information security. This means that information security obligations in legislation also affects other areas.

The analysis of the act against the service production and service output helped with the comparison work between the new act and the previous decree. This comparison was carried out to find out if there is a possibility to use the concurrent requirements or if the change in legislation needs more extensive renewal. The results showed that even though the new legislation had some completely new issues, some of the content and obligations would be comparable with the previous legislation and the content of previous requirements could be used.

The final part of this thesis was to create a suitable template for a single requirement. Then, based on the research and analysis, information security requirements used in IT procurements were renewed by using this new template. The main observations during this part were the overlapping between the security agreement and concurrent information security requirements and the lack of cohesion in concurrent software development requirements, which led to add-on security thinking instead of built-in security thinking.

The significance of this thesis to the Legal Register Centre was big. The Legal Register Centre is responsible for the development and maintenance of the information systems under the Ministry of Justice and therefore it accomplishes public IT procurements constantly. There were no official recommendations for authorities available to guide the enforcement of new legislation at the time it became obligatory. Therefore, the notability of this thesis was emphasised by the assigner of this thesis. The first recommendations were published in April 2020.

At the time of writing this thesis, the updated information security requirements have already been a part of at least four IT procurements arranged by the Legal Register Centre. Some of them are already completed and the work has already started, and some of them are under definition phase.

The first experience of the use the requirements has been encouraging. Many stakeholders have found the new model clear, with the title, description and verification instructions. Also, the lesser number of requirements has been found positive.

This model has been presented cross-administratively in central government. Some agencies have already taken the model into use.

Even though the start for this model has been encouraging, the model is not ready yet. Most of the persons defining the subject-matter has no knowledge about information security. Therefore, this model should be developed to better guide and support these persons in their definition work and to find the dependencies to information security. Guidance and procedures should also be developed to help the customer, i.e. the authority, to monitor if service development and service output are fulfilling the obligations set in information management requirements even though they now include verification instructions.

Additionally, the requirements cover now only a customised information system. There is need to add other parts as well. More and more suppliers are moving their services from data centres to cloud environment so this might be the next big target for development.

References

Act 625/2012 *Laki Oikeusrekisterikeskuksesta* [Act on Legal Register Centre]. Accessed on 16 January 2020. Retrieved from https://www.finlex.fi/fi/laki/ajantasa/2012/20120625

Act 1397/2016 *Laki julkisista hankinnoista ja käyttöoikeussopimuksista* [Act on Public Contracts and Concessions]. Accessed on 2 February 2020. Retrieved from https://www.finlex.fi/fi/laki/ajantasa/2016/20161397

Act 906/2019 *Laki julkisen hallinnan tiedonhallinnasta* [Act on Information Management in Public Administration]. Accessed on 16 January 2020. Retrieved from https://www.finlex.fi/fi/laki/alkup/2019/20190906

Act 906/2019 (English version). *Act on Information Management in Public Administration*. Accessed on 16 January 2020. Retrieved from https://www.finlex.fi/fi/laki/kaannokset/2019/en20190906

Aukia, J-P. 2018. *Oikeuslaitoksen tietojärjestelmät – renkejä vai isäntiä?* [Information systems of the judiciary – hired hands or masters?]. Lakimiesuutiset. Accessed on 2 February 2020. Retrieved from https://lakimiesuutiset.fi/ovatko-oikeuslaitoksen-tietojarjestelmat-renkeja-vai-isantia/

Decree 681/2010 (English version). *Government Decree on information security in central government*. Accessed on 16 January 2020. Retrieved from https://www.finlex.fi/en/laki/kaannokset/2010/en20100681

DVV (Digital and Population Data Services Agency). N.d. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI [Public Administration Digital Security Management Board VAHTI]. Web page. Accessed on 14 April 2020. Retrieved from https://dvv.fi/vahti

Finlex. N.d. *Legislative Drafting Process Guide*. Web page. Accessed on 10 February 2020. Retrieved from http://lainvalmistelu.finlex.fi/en/

Finnish Government. 2018. *Hallituksen esitys VM/2018/201* [Government bill VM/2018/201] Accessed on 10 February 2020. Retrieved from https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f805f1863

Government Strategy Secretariat. 2018. *Finland, a land of solutions: Government Action Plan 2018–2019*. Finnish government publication series 29/2018. Prime Minister's Office. Accessed on 24 March 2020. Retrieved from http://julkaisut.valtioneuvosto.fi/handle/10024/160985

Haikala, I. & Mikkonen, T. 2011. *Ohjelmistotuotannon käytännöt* [Practices of the software engineering]. 12th. ed., Rev. ed. Hämeenlinna: Talentum Media.

Hartig, O. 2014. *Tieto kehitti tuomioistuimille sovelluksen - toiminta hidastui, budjetti ylittyi ja aikataulu venyi* [Tieto developed application to the courts - operation slowed down, budget and schedule exceeded]. Tietoviikko. Accessed on 2 February 2020. Retrieved from https://www.tivi.fi/uutiset/tieto-kehitti-tuomioistuimille-sovelluksen-toiminta-hidastui-budjetti-ylittyi-ja-aikataulu-venyi/2c1f414d-9d76-3319-a13c-7f06b38bd892

HE 284/2018 Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi [Government bill to Parliament of Finland for Act on Information Management in Public Administration and for some related acts]. 2018. Accessed on 16 January 2020. Retrieved from http://finlex.fi/fi/esitykset/he/2018/20180284

ISO/IEC/IEEE 24765. 2017. *Systems and software engineering -- Vocabulary*. 2nd ed. Accessed on 10 April 2020. Retrieved from https://janet.finna.fi, IEEE Xplore Digital Library. doi: 10.1109/IEEESTD.2017.8016712

ISO/IEC/IEEE 29148. 2018. *Systems and software engineering -- Life cycle processes -- Requirements engineering*. 2nd ed. Accessed on 10 April 2020. Retrieved from https://janet.finna.fi, IEEE Xplore Digital Library. doi: 10.1109/IEEESTD.2018.8559686

Koski, A., 2019. *On the Provisioning of Mission Critical Information Systems based on Public Tenders*. Doctoral thesis. University of Helsinki, Faculty of Science, Computer Science. Accessed on 7 January 2020. Retrieved from http://urn.fi/URN:ISBN:978-951-51-5325-8 (https://helda.helsinki.fi/handle/10138/303511)

Kuuttiniemi, K., Lehtomäki, L. 2017. *Valtion hankintakäsikirja 2017* [Handbook on Government Procurements 2017]. Ministry of Finance publications 29/2017. Helsinki: Ministry of Finance. Accessed on 9 February. Retrieved from https://vm.fi/julkaisu?pubid=20801

Legal Register Centre. 2019. Page on Legal Register Centre's webpage. Accessed on 5 February. Retrieved from https://www.oikeusrekisterikeskus.fi/en/index/loader.html.stx?path=/channels/public/www/ork/en/structured_nav/oikeusrekisterikeskus

Ministry of Finance. 2016. *Tiedonhallinnan lakiuudistus avoimella valmistelulla* [Reform of information management legislation in open preparation]. Bulletin published on 22 November 2016 on the web page of the Ministry of Finance. Accessed on 10 February 2020. Retrieved from https://vm.fi/artikkeli/-/asset_publisher/tiedonhallinnan-lakiuudistus-avoimella-valmistelulla

Ministry of Finance. 2017a. *Tiedonhallintaa koskevaa yleistä sääntelyä on kehitettävä* [General regulation concerning information management must be improved]. Bulletin published on 29 September 2017 on the web page of the Ministry of Finance. Accessed on 10 February 2020. Retrieved from https://vm.fi/artikkeli/-/asset_publisher/tiedonhallintaa-koskevaa-yleista-saantelya-on-kehitettava

Ministry of Finance. 2017b. *Lausuntopyyntö julkisen hallinnon tiedonhallinnan sääntelyn kehittämistä selvittäneen työryhmän raportista* [Request for comments concerning the report by work group researching the regulation of information management in public administration]. Accessed on 10 February 2020. Retrieved from https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=7ce3c761-d472-4d45-9f1a-3adae6b6604a

Ministry of Finance. 2018a. *Tiedonhallintalain valmistelu jatkuu hallitusohjelman tavoitteiden mukaisesti.* [Preparation of the information management act continues in accordance with requirements of Government programme]. Bulletin published on 11 January 2018 the web page of the Ministry of Finance. Accessed on 10 February 2020. Retrieved from https://vm.fi/artikkeli/-/asset_publisher/tiedonhallintalain-valmistelu-jatkuu-hallitusohjelman-tavoitteiden-mukaisesti

Ministry of Finance. 2018b*. Luonnos hallituksen esitykseksi eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi* [Draft of Government bill to Parliament of Finland for Act on Information Management in Public Administration and for some related acts]. Accessed on 10 February 2020. Retrieved from https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=3010f613-2ede-40c1-a59f-e75c23cddbb5

Ministry of Finance. 2020a. *Uusi tiedonhallintalautakunta on asetettu edistämään tiedonhallinnan kehittämistä julkisessa hallinnossa* [New Information Management Board was set up for enhancing the development of information management in public administration]. Bulletin published on 27 January 2020 on the web page of the Ministry of Finance. Accessed on 13 April 2020. Retrieved from https://vm.fi/artikkeli/-/asset_publisher/uusi-tiedonhallintalautakunta-on-asetettu-edistamaan-tiedonhallinnan-kehittamista-julkisessa-hallinnossa

Ministry of Finance. 2020b. Julkisen hallinnon digitaalinen turvallisuus [Digital security in public administration]. Publications of the Ministry of Finance 2020:23. Accessed on 13 April 2020. Retrieved from http://urn.fi/URN:ISBN:978-952-287-857-1

Ministry of Finance. N.d. Digitaalisen turvallisuuden strateginen johtoryhmä [Strategic Management Group for Digital Security]. Web page. Accessed on 13 April 2020. Retrieved from https://vm.fi/hanke?tunnus=VM025:00/2020

Parliament of Finland. 2019. *HE 284/2018 vp*. Accessed on 24 March 2020. Retrieved from https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_284+2018.aspx

Pekkala, E., Pohjonen, M., Huikko, K. & Ukkola, M. 2019. *Hankintojen kilpailuttaminen ja sopimusehdot* [Tendering the procurements and contract terms]. 8th. Rev. ed (10th. ed.). Tallinna: Tietosanoma.

Prime Minister's Office. 2015. *Finland, a land of solutions - Strategic Programme of Prime Minister Juha Sipilä's Government 29 May 2015*. Government Publications 12/2015. Helsinki: Ministry of Finance. Accessed on 7 January 2020. Retrieved from https://vm.fi/julkaisu?pubid=6407

Rautenbach, W. J., de Kock, I & Jooste, J. L. 2019. *The development of a conceptual model for enabling a value-adding digital transformation: A conceptual model that aids organisations in the digital transformation process*. IEEE. Accessed on 7 January 2020. Retrieved from https://janet.finna.fi, IEEE Xplore Digital Library. doi: 10.1109/ICE.2019.8792675

Robertson, S. & Robertson, J. 2014. *Mastering the Requirements Process: Getting Requirements Right*. 3rd. ed., Addison-Wesley. E-book.

Sathananthan, S., Hoetker, P., Gamrad D., Katterbach, D. & Myrzik, J. 2017. *Realizing digital transformation through a digital business model design process*. IEEE. Accessed on 7 January 2020. Retrieved from https://janet.finna.fi, IEEE Xplore Digital Library. doi: 10.1109/CTTE.2017.8260996.

Security Committee. 2019. *Finland's Cyber Security Strategy 2019*. Helsinki: Author. Accessed on 16 January 2020. Retrieved from https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/

Storås, N. 2014. *It-hanke epäonnistui täysin - Tiedolla oli "sisäisiä haasteita ja kommunikaatio-ongelma"* [IT project failed completely - Tieto had “internal challenges and communication problems]. Tietoviikko. Accessed on 13 February 2020. Retrieved from https://www.tivi.fi/uutiset/it-hanke-epaonnistui-taysin-tiedolla-oli-sisaisia-haasteita-ja-kommunikaatio-ongelma/8e27a630-0753-3f33-ac0c-61c4ad6632cb

Vänskä, O. 2017. *Paholaisen tusina: 13 epäonnista it-projektia - näihin poltettiin Suomessa miljoonia* [Devil's dozen: 13 unfortunate it-projects - millions were wasted for them in Finland]. Tietoviikko. Accessed on 2 February. Retrieved from https://www.tivi.fi/uutiset/paholaisen-tusina-13-epaonnista-it-projektia-naihin-poltettiin-suomessa-miljoonia/8691e95b-f7fe-36ee-913d-be1edf71e72e

Appendices

Appendix 1. Supporting questions

This appendix includes examples of supporting questions. They can be used for eliciting the information security related needs which can then, after analysis, be written as information security requirements. The list is not supposed to be exhaustive. The meanings of the questions are also shortly explained later.

1. How critical the information system is? How long is it possible to operate without it?
2. What kind of data it is stored and processed in the information system?
    a. Public data
    b. Confidential data
    c. Personal data
3. In what geographical location the data of the information system can be located?
    a. Only in Finland
    b. Only in EU (European Union)
    c. In EU and EEA (European Economic Area)
    d. In EU, EEA and third countries under GDPR
4. What kind of tasks the supplier is performing? What are the supplier's roles in service production?
5. Does the supplier get access to the authority's confidential data related to information system and its development or similar?
    a. Any requirements for premises, network connections or equipment?
    b. Any requirements for storing confidential data?
6. Does the supplier get access to productive environment?
    a. What kind of tasks the supplier is performing there? In what roles?
    b. Are separate safety premises required to perform these tasks? Requirements for network connections or for equipment? Other?
7. In what geographical location the supplier can produce service? Includes the location of supplier's supporting systems for service production and data in them.
    a. Only in Finland
    b. Only in EU
    c. In EU and EEA
    d. In EU, EEA and third countries under GDPR
8. Does the information system offer digital service for citizens?
    a. What kind of data can be accessed, public or confidential?
    b. Does the service require login?
    c. Does the citizen have a possibility to send files to system via service?
9. Does the information system have integrations to other information systems?
    a. Does the traffic between the systems go through public network or internal network?
    b. Does the target system belong to own organisation or other organisation?
    c. Is target system sender or receiver?
    d. What kind of data is sent/received?
    e. Is the classification of data in the same level in both systems?

Question 1 helps to analyse the level of continuity. More critical the system is more carefully the continuity and related measures, for example mirroring the system and requirement to test restoring, need to be planned.

Question 2 helps to identify what kind of data is stored and processed in system. It needs to be noted that security classified data (national and international) is missing from the list. Personal data which is used in criminal matters and in connection with maintaining national security is missing too.

Question 3 is related to question 2. The possible geographical location of data is related to the content and classification of data.

Questions 4-7 help to identify the need to require possible security clearances for employees of the supplier. It is dependent on the roles and tasks of the employees and the data they have access. These issues can also set requirements for premises, data network and connections, equipment and geographical location of service production and its supporting systems.

Question 8 is for digital services. The information system measures are dependent on the service and the data and its classification. For example, if there is possibility to send files, there needs to be protection against malware and if the citizen has access to his or her personal data the identification must be strong enough.

Question 9 helps to identify if there are any integration to other systems and for whom they belong. Depending on data and network it can set need for encryption and protection against malware. There might be also need for identification of system with certificates. If the classification of systems differs there might be a need to use boundary protection service.

Appendix 2. Information security requirements (in Finnish)

Toimittaja sitoutuu täyttämään kaikki tämän asiakirjan vaatimukset. Tilaajalla on oikeus auditoida palvelu itse tai kolmannen osapuolen toimesta.

1. Palvelun tuottamiseen liittyvät tietoturvallisuusvaatimukset

Mikäli muuta ei mainita, Toimittajan tulee suorittaa tässä luvussa kuvatut toimenpiteet, jotka kohdistuvat hankinnan kohteen palvelun tuottamiseen, jäljempänä ’palvelu’.

Toimittaja laatii tässä luvussa vaaditut kirjalliset kuvaukset sopimuskauden alussa.

Toimittaja laatii ja toimittaa tässä luvussa vaaditut raportit Tilaajan ja Toimittajan yhdessä, sopimuskauden alussa sovittujen käytänteiden mukaisesti, mikäli yksittäisessä vaatimuksessa ei toisin sanota.

1.1 Toimittaja kuvaa kirjallisesti palvelun turvallisuusperiaatteet ja nimeää palvelun vastuuhenkilöt.

Toimittaja kuvaa kirjallisesti turvallisuusperiaatteet, joita Toimittaja noudattaa tuottaessa palvelua ja käsitellessään palveluun liittyvää tietoa. Turvallisuusperiaatteissa on huomioitava palveluun ja sen jatkuvuuteen oleellisesti vaikuttavat sisäiset ja ulkoiset tekijät. Turvallisuusperiaatteiden tulee kattaa kaikki palvelun osa-alueet ja täyttää Tilaajan vaatima taso.

Lisäksi Toimittaja kuvaa turvallisuusperiaatteissa palvelun tietoturvallisuuden, jatkuvuuden ja tietosuojan seuraamiseen ja kehittämiseen liittyvät tehtävät ja roolit sekä niiden vastuut. Toimittaja nimeää näihin rooleihin vastuu- ja varahenkilöt.

Turvallisuusperiaatedokumentin toteutus- ja tallennusmuoto sovitaan yhteisesti sopimuskauden alussa. Toimittaja hyväksyttää tietoturvamenettelyn Tilaajalla.

Vaatimus todennetaan siten, että sopimuskauden alussa Toimittaja kuvaa kirjallisesti palvelun turvallisuusperiaatteet ja toimittaa Tilaajalle hyväksyttäväksi. Hyväksymisestä on hyväksymismerkinnät yhteisesti sovitulla tavalla.

Lisäksi Toimittaja varmistaa, että Tilaajalla on ajantasainen lista vastuuhenkilöistä ja heidän varahenkilöistään.

1.2 Toimittaja valvoo ja parantaa palvelun tuottamisen tietoturvallisuutta.

Toimittaja valvoo jatkuvasti, että palvelun tuottamisessa noudatetaan tietoturvallisuudesta annettuja ohjeita ja puuttuu välittömästi havaitsemiinsa tai sen tietoon tulleisiin poikkeamiin ja kirjaa ne.

Toimittajan tulee myös jatkuvasti seurata mahdollisia muutoksia tietoturvallisuuskentällä sekä arvioida muutosten vaikutusta palvelun turvallisuusperiaatteiden kattavuuteen ja riittävyyteen, jotta Toimittaja pystyy ylläpitämään sovitun turvallisuustason. Toimittajan tulee tarvittaessa ryhtyä arvioinnin perusteella korjaaviin toimenpiteisiin omalla kustannuksellaan. Mikäli joistakin toimenpiteistä aiheutuu kustannuksia Tilaajalle, Toimittajan tulee hyväksyttää ne Tilaajalla erikseen. Arviointitulokset ja muutostoimenpiteet tulee dokumentoida.

Lisäksi Toimittaja ja Tilaaja kokoontuvat säännöllisesti arvioimaan yhdessä palvelun tietoturvallisuuteen tilannetta ja palveluun liittyviä tietoturvallisuusriskejä. Samalla osapuolet sopivat yhteisesti arvioinnin tulosten perusteella suoritettavista kehittämistoimenpiteistä ja sopivat vastuutahot. Osapuolet sopivat myös mahdollisesta kustannusten jakamisesta. Lisäksi osapuolet seuraavat aiemmin sovittujen toimenpiteiden edistymistä.

Tilaaja ja Toimittaja sopivat säännöllisistä kokoontumisista ja niiden tarkemmista sisällöistä yhteisesti sopimuskauden alussa.

Vaatimus todennetaan siten, että Toimittaja pystyy pyydettäessä osoittamaan, että henkilöstölle on annettu palvelun tuottamisen liittyvää tietoturvallisuusohjeistusta ja että Toimittaja valvoo ohjeiden noudattamista ja kirjaa havaitut ja ilmoitetut poikkeamat.

Toimittaja esittää Tilaajalle säännöllisesti, kuitenkin vähintään kerran vuodessa, palveluun liittyvän tietoturvallisuuden arvioinnin tulokset ja sen perusteella esiin nousseet ja tehdyt kehittämis- ja korjaustoimenpiteet.

Lisäksi Toimittaja osallistuu yhteistyössä Tilaajan kanssa palveluun liittyvien tietoturvallisuusriskien arviointiin yhdessä sovitun mukaisesti.

1.3 Toimittaja vastaa, että palvelun tuottamiseen osallistuva henkilöstö on koulutettu tehtäviinsä.

Toimittaja vastaa siitä, että palvelun tuottamiseen osallistuva henkilöstö on koulutettu rooliensa mukaisiin tehtäviinsä.

Toimittaja kouluttaa palvelun tuottamiseen osallistuvaa henkilöstöä säännöllisesti myös tietoturvallisuuden ja tietosuojan sekä niihin liittyvien ajantasaisten käytäntöjen osalta, jotta palvelun tuottamisen tietoturvallisuuden taso pysyy vähintään Tilaajan määrittämällä tasolla.

Toimittajan tulee kehittää ja ylläpitää palvelun tuottamiseen osallistuvan henkilöstön osaamista, jotta palvelun taso pysyy vähintään sovitulla tasolla.

Tilaaja sitoutuu ilmoittamaan Toimittajalle välittömästi, mikäli palvelun kohteeseen liittyvä lainsäädäntö, ohjeet tai käytännöt muuttuvat. Toimittaja sitoutuu tiedottamaan edellä mainituista Tilaajan ilmoittamista muutoksesta palvelun tuottamisesta vastaavalle henkilöstölleen sekä alihankkijoilleen palvelun tuottamisen edellyttämässä laajuudessa.

Vaatimus todennetaan siten, Toimittaja pystyy osoittamaan palvelun tuottamiseen osallistuvan henkilöstön kouluttamisen.

Lisäksi Toimittaja pystyy tarvittaessa osoittamaan, että on tiedottanut henkilöstöä ja tarvittaessa alihankkijoita muuttuneista ohjeista ja käytännöistä sekä palvelua koskevan lainsäädännön muuttumisesta.

1.4 Toimittaja reagoi palveluun kohdistuviin turvallisuushäiriöihin viivytyksettä ja raportoi niistä Tilaajalle.

Turvallisuushäiriöillä tarkoitetaan tässä kaikkia palvelun turvallisuuteen liittyviä häiriöitä ja niihin sisältyvät myös tietoturvaan ja tietosuojaan sisältyvät häiriöt ja poikkeamat.

Toimittajalla on menettelytavat palveluun kohdistuvien turvallisuushäiriöiden käsittelyyn ja raportointiin. Toimittaja on myös nimennyt henkilöt turvallisuushäiriöiden hallintaan.

Toimittaja on myös määritellyt selkeät menettelyt turvallisuushäiriöiden ilmoittamiseen ja on ohjeistanut ja kouluttanut ne palvelun tuottamiseen osallistuvalle henkilöstölle.

Menettely huolehtii myös siitä, että palveluun liittyvien sähköisten viestien, sähköpostien, tunnistamistietojen sekä paikkatietojen luottamuksellisuudesta ja oikeasta käsittelystä myös tietoturvapoikkeamatilanteita selvitettäessä

Toimittaja reagoi tietoturvapoikkeamiin viivytyksettä ja ryhtyy niiden johdosta tarvittaviin toimenpiteisiin. Toimittaja pitää kirjaa tietoturvapoikkeamista ja raportoi ne Tilaajalle.

Hankinnan kohteeseen liittyvien henkilötietojen vaarantuminen on aina vakava poikkeama, josta Toimittajan on ilmoitettava Tilaajalle viivytyksettä.

Toimittaja huolehtii myös siitä, että hankinnan kohteen tuottamiseen osallistuva henkilöstö tietää, kenelle hankinnan kohteeseen kohdistuvista tietoturvapoikkeamista ja -tapahtumista tai niiden uhkista tulee ilmoittaa.

Vaatimus todennetaan siten, että Toimittaja pystyy pyynnöstä esittämään menettelyn palveluun liittyvien turvallisuushäiriöiden käsittelyyn ja raportointiin ja että sitä noudatetaan palvelun tuottamisessa.

Lisäksi Toimittaja pystyy tarvittaessa osoittamaan, että se on tiedottanut palvelun tuottamiseen osallistuvaa henkilöstöä siitä, kenelle turvallisuushäiriöistä tai niiden uhista tulee ilmoittaa.

Toimittaja raportoi turvallisuushäiriöistä Tilaajalle.

1.5 Toimittaja vastaa luottamuksellisen ja salassa pidettävän aineiston tietoturvasta ja tietosuojasta aineiston koko elinkaaren ajan.

Toimittaja antaa palveluun liittyvän luottamuksellisen ja salassa pidettävän aineiston vain niiden henkilöiden saataville, jotka tarvitsevat sitä palvelun tuottamisessa, ja jotka täyttävät Turvallisuussopimuksessa mainitut edellytykset salassa pidettävän aineiston käsittelyyn.

Toimittaja huolehtii myös, että kyseiset henkilöt tietävät, miten aineistoa koskevasta tietoturvallisuudesta ja tietosuojasta huolehditaan aineiston koko elinkaaren ajan.

Vaatimus todennetaan siten, että Toimittaja ylläpitää luetteloa palveluun liittyvää salassa pidettävää tietoa käsittelevistä henkilöistä ja pystyy pyynnöstä esittämään luettelon.

Lisäksi Toimittaja pystyy osoittamaan, että on ohjeistanut kyseiset henkilöt huolehtimaan luottamuksellisen ja salassa pidettävän aineiston tietoturvallisuudesta ja tietosuojasta aineiston koko elinkaaren ajan.

1.6 Toimittaja huolehtii vastuullaan olevista palvelun tuottamiseen käytettävistä ICT-resursseista ja niiden tietoturvallisuudesta.

Toimittaja organisoi ja vastuuttaa vastuullaan olevien palvelun tuottamiseen käytettävien ja liittyvien fyysisten ja virtuaalisten laitteiden, tietojärjestelmien, palveluiden ja ohjelmistojen luetteloinnin ja kuvausten laadinnan sekä em. luetteloiden ja kuvausten ylläpidon.

Kuvauksissa tulee ilmetä myös edellä mainittuihin ICT-resursseihin mahdollisesti liittyvät yhteydet julkiseen tietoverkkoon (Internet) ja mitä tietoja näiden yhteyksien kautta toimitetaan. Lisäksi kuvauksista tulee ilmetä, missä maantieteellisissä sijainneissa tallennettu tieto sijaitsee, koskien myös mahdollisia pilvipalveluita.

Toimittaja luetteloi myös palvelun tuottamiseen käytettävät ohjelmisto- ym. lisenssit, ja ylläpitää luetteloa.

Lisäksi Toimittaja organisoi ja vastuuttaa edellä mainittujen ICT-resurssien päivitys- ja muutostarpeiden seurannan, päivityspäätösten teon ja päivitysten asennuksen erityisesti tietoturvapäivitysten osalta.

Toimittaja raportoi edellä mainittujen vastuullaan olevien ICT-resurssien ja niiden hallinnan tietoturvallisuuden tilasta Tilaajalle säännöllisesti, vähintään kerran vuodessa.

Vaatimus todennetaan siten, että Toimittaja pystyy osoittamaan, että on organisoinut ja vastuuttanut vastuullaan olevien palvelun tuottamiseen käytettävien ICT-resurssien luetteloinnin ja kuvausten laadinnan, ja pystyy pyydettäessä toimittamaan luettelot ja kuvaukset.

Lisäksi Toimittaja pystyy todentamaan, että edellä mainittujen ICT-resurssien päivitys- ja muutostarpeita seurataan.

Toimittaja raportoi Tilaajalle vaatimuksen mukaisesti säännöllisesti, vähintään kerran vuodessa

2. Palvelun tuloksena olevan tietojärjestelmään ja sen kehittämiseen liittyvät tietoturvallisuusvaatimukset

Tietojärjestelmän tulee täyttää tässä luvussa olevat sovelluskehityksessä huomioitavat tietoturvavaatimukset.

Tietojärjestelmässä tulee voida käsitellä sekä henkilötietoja että salassa pidettävää aineistoa.

2.1 Toimittaja suunnittelee ja kehittää verkkosovelluksen ajantasaisia tietoturvakäytänteitä noudattaen.
Toimittaja suunnittelee ja toteuttaa verkkosovelluksen ajantasaisia OWASP Top 10 -käytänteitä noudattaen. Käytänteet on listattu liitteessä Liite_X_OWASP_Top_10_2017.pdf. Liite on englanninkielinen. Toimittaja suunnittelee ja toteuttaa verkkosovelluksen ulospäin näkyvät rajapinnat ajantasaisia OWASP API Top 10 -käytänteitä noudattaen. Käytänteet on listattu liitteessä Liite_Y_OWASP_API_Security_Top_10_2019.pdf. Liite on englanninkielinen. Liitteen X lähde: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf (viitattu 14.11.2019). Liitteen Y lähde: https://github.com/OWASP/API-Security/raw/master/2019/en/dist/owasp-api-security-top-10.pdf (viitattu 1.4.2020).
Vaatimus todennetaan siten, että Toimittaja pystyy pyydettäessä esittämään liitteissä kuvattujen tietoturvakäytänteiden huomioimisen koko sovelluskehittämisen toteutusketjussa suunnittelusta testaukseen ja verkkosovelluksen julkaisuun.

2.2 Toimittaja laatii tietotojärjestelmän lokitussuunnitelman ja toteuttaa lokituksen sen mukaisesti.

Toimittaja laatii tietojärjestelmän lokitussuunnitelman yhteistyössä Tilaajan kanssa ja toteuttaa tietojärjestelmän lokituksen sen mukaisesti. Teknisen lokituksen lisäksi lokituksessa tulee huomioida ns. audit trail. Lokitussuunnitelma tulee versioida.

Toimittaja toteuttaa tietojärjestelmän lokien lähettämisen Tilaajan hallinnoimaan keskitettyyn lokienhallintajärjestelmään Tilaajan ohjeistuksen mukaisesti.

Toimittaja ylläpitää lokitussuunnitelmaa ja tekee siihen tarvittavat muutokset lokitustarpeen muuttuessa.

Vaatimus todennetaan siten, että Tilaaja suorittaa itsenäisesti tai kolmannen osapuolen toimesta lokituksen tarkastuksen, jossa toteutettua lokitusta verrataan lokitussuunnitelman uusimpaan versioon.

2.3 Toimittaja seuraa ja ylläpitää vastuullaan olevien ympäristöjen tietoturvallisuutta, joita käytetään tietojärjestelmän kehittämiseen.

Toimittaja ylläpitää listaa vastuullaan olevista, tietojärjestelmän kehittämiseen käytettävistä, kehitys- ja testiympäristöistä ja niiden ohjelmistoista versiotietoineen.

Toimittaja seuraa edellä mainittujen ympäristöjen ja ohjelmistojen haavoittuvuus- ja tietoturvapäivitysilmoituksia ja analysoi ympäristöjen päivitystarpeen riippuvuuden huomioiden.

Lisäksi Toimittaja laatii analyysin perusteella päivityksille päivityssuunnitelman aikatauluineen ja päivittää ympäristöt sen mukaisesti.

Toimittaja huolehtii siitä, että tietojärjestelmän kehittämiseen käytettävien ympäristöjen ohjelmistoversioiden (käyttöjärjestelmä ja sovellukset) ovat aktiivisten tuen ja päivitysten piirissä.

Vaatimus todennetaan siten, että Toimittajalla on nimetty vastuuhenkilö ylläpitämään listaa Toimittajan vastuulla olevien ympäristöjen haavoittuvuus- ja tietoturvapäivitysten seurantaan ja tietoturvapäivitysten asennusten tekemiseen.

2.4 Toimittaja testaa verkkosovelluksen tietoturvallisuuden vaatimustenmukaisuuden.
Toimittaja suunnittelee ja toteuttaa sekä manuaalista että automatisoitua tietoturvatestausta verkkosovelluksen sovelluskehitystyön eri vaiheissa. Toimittaja ei saa käyttää testiaineistona dataa, joka sisältää aitoja henkilötietoja tai salaiseksi luokiteltuja tietoja. Toimittaja laatii ja ylläpitää testausta varten oikeamuotoista mutta keinotekoista testiaineistoa. Lisäksi Toimittajan tulee testata verkkosovelluksen tietoturvallisuus käyttäen OWASP Application Security Verification Standardin version 4.0 tasoa 2 (L2) soveltuvin osin. (* Käytettävä standardi on liitteenä Liite_Z_OWASP_ASVS_4.0.pdf. Liite on englanninkielinen. Liitteen Z lähde: https://github.com/OWASP/ASVS/raw/master/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0-en.pdf (viitattu 14.11.2019). *) Kryptografiasuosituksissa noudatetaan OWASP:n suosituksista poiketen kansallisia ja ajantasaisia NCSA-FI -suosituksia.
Vaatimus todennetaan siten, että Toimittajalla on nimetty vastuuhenkilö ylläpitämään listaa Toimittajan vastuulla olevien ympäristöjen haavoittuvuus- ja tietoturvapäivitysten seurantaan ja tietoturvapäivitysten asennusten tekemiseen.

2.5 Toimittaja tuottaa tietojärjestelmän asennukseen, päivittämiseen, palauttamiseen ja ylläpitoon liittyvää ohjeistusta.

Toimittaja tuottaa tietojärjestelmän asennuksesta, varmuuskopioinnista, palautuksesta, versionvaihdosta ja poistamisesta sekä muista mahdollisista sovelluksen asennukseen ja ylläpitoon liittyvistä töistä ohjeet ja toimittaa ne sekä Tilaajalle että järjestelmän asennuksesta ja ylläpidosta vastaavalle taholle. Toimittaja päivittää ohjeita tarpeen mukaan ja toimittaa päivitetyt versiot edellä mainituille tahoille.

Toimittaja laatii myös jokaiseen julkaistavaan ohjelmistoversioon julkaisutiedotteen (release notes) ja toimittaa sen Tilaajalle ja asennuksesta vastaavalle taholle.

Lisäksi toimittaja osallistuu omalta osaltaan Tilaajan kanssa yhteistyössä tehtävän toipumissuunnitelman ja palvelukuvauksen tekemiseen ja ylläpitoon.

Vaatimus todennetaan siten, että Toimittaja laatii vaatimuksessa kuvatut ohjeet ja toimittaa ne Tilaajalle ja asennuksesta ja ylläpidosta vastaavalle taholle.

Lisäksi Toimittaja osallistuu toipumissuunnitelman ja palvelukuvauksen laatimiseen yhdessä Tilaajan kanssa.

2.6 Toimittajalla on menettelyt sekä tietojärjestelmään liittyvien vaatimusten ja toiminnallisuuksien jäljitettävyyteen ja muutoshallintaan.

Toimittajalla on laadittuna menettelyt tietojärjestelmän vaatimusten ja toiminnallisuuksien jäljitettävyyteen.

Toimittajalla on myös menettely vaatimusten ja toiminnallisuuksien muutoshallintaan.

Toimittaja käyttää ohjelmistokehittämisessä versionhallintaa.

Vaatimus todennetaan siten, että Toimittaja pystyy esittämään jäljitettävyyteen, muutoshallintaan ja versionhallintaan liittyvät menettelyt.

Lisäksi Tilaaja suorittaa itsenäisesti tai kolmannen osapuolen toimesta vaatimuksiin tai toiminnallisuuksiin liittyvien jäljitettävyysketjujen tarkastuksen.