Turun yliopisto
University of Turku

# PIECES OF A PUZZLE

## Exploring information security services

Master´s Thesis
in Information Systems Science

Author:
Lotta Kulta

Supervisors:
Ph.D. Jani Koskinen
Dr. Sc. Jonna Järveläinen

15.12.2017
Turku

# Table of contents

## List of figures

## List of tables

# 1 INTRODUCTION

For the purpose of this study, it is vital to understand the current field of information security (later infosec) and its challenges towards the society and its organizations in particular. This introductory section will begin by illustrating the importance of information security to organizations, which will then be followed by some real life examples of information security breaches. In the final part of this section, the structure of the thesis will be presented as a stepping stone to the next sections of the study.

## 1.1 Motivation

Due to the rapid digitalization of products and services, individuals are becoming more and more connected in their everyday life. This sets new demands on companies and other organizations as the increasing connectedness predisposes both businesses and individuals to information security threats. Consequently, it is important to notice, that these threats do not only risk the information security of organizations but also the privacy and security of their customers and suppliers. In fact, to tackle this issue, the European Union is launching a new data protection regulation. The new EU general data protection regulation (GDPR) brings companies greater responsibility over the protection of customer data (Hartikainen 2016): violations of the regulation could lead to sanctions as high as 20 million EUR or 4.0% of the annual global revenue of the company (EU-tietosuojan kokonaisuudistus 2016, 6–7). This can be seen as an important change, as data protection supervisor Reijo Aarnio estimates that companies still have much room for improvement in the data protection field (Hartikainen 2016). In fact, according to the Finnish Communications Regulatory Authority and its National Cyber Security Center, there have been several extortion malware infections in Finnish companies and hospitals in spring 2016 (Rissanen & Koivuranta 2016). Furthermore, in a study conducted by the consulting company KPMG in 10 Finnish publicly listed companies in 2013, nearly half of the companies had Trojan virus in their data-communications networks, one third other malware and, additionally, the networks of four companies had been hacked (Halminen 2014). What is even more alarming is, that in spring 2016, a content management system utilized by several governmental sites, such as the Ministry of Finance, the Finnish Defence Forces, the Ministry of Social Affairs and Health and the Family Federation of Finland was subjected to a denial of service (DOS) attack (Ministeriöiden verkkopalveluihin hyökättiin jälleen 2016).

In the business field, on the other hand, the web services provider Yahoo was subjected to two information security breaches in 2013 and 2014 that lead to the theft of customer names, email addresses, phone numbers and passwords of over a billion customers. Due

to the breaches, Verizon, who acquired parts of Yahoo, was able to lower the purchase price of the company by 350 million dollars. (Linnake 2017.) The victims of the theft included employees of the civil and military administration of the United States, members of the White House, federal police officers, congressmen and intelligence authorities from the US and, therefore, in the hands of cyber criminals, the information could lead to severe national threat to the United States. This has been said to be the largest information security breach in the world. (Yahoolta uusi paljastus – – 2016.) Furthermore, in spring-summer 2017, two global ransomware attacks that affected companies worldwide – WannaCry and Petya – were launched causing serious impacts. Petya affected multiple organizations in the fields of shipping and transport, pharmaceuticals and oil production, in addition to impacting the airport, power grid and governmental bodies in Ukraine, whereas WannaCry locked up over 200 000 companies worldwide (Ng 2017). Moreover, WannaCry is said to have affected computers in over 150 countries (Virtanen 2017); impacted organizations include hospitals including National Health Service NHS in UK, universities, banks and railways, governmental bodies and automobile, transport, telecom and gas companies around the globe to name a few (Ransomware cyber-attack – – 2017). These examples highlight the importance of information security in different levels of the society and demonstrate that information security is a topic no longer to be neglected by any organization.

Meanwhile, the global cyber security market is valued at over $120 billion in 2017 and investments in the area between years 2017 and 2021 are expected to cumulatively exceed $1 trillion (Morgan 2017). There is a plethora of companies offering products, services and solutions related to information security both in Finland and abroad. These solutions come in handy as the study conducted by CGI (CGI – – 2016; 1, 8) demonstrated that 86% of the respondents of the study felt that the risk of a cyber attack had increased within a year and, in fact, 74% of respondents saw it likely that they will be subjected to a cyber security attack within the next year. Furthermore, 63% of respondents saw it as likely that the organization had suffered from a cyber attack without anyone knowing it. Consequently, 81% of the organizations recognize that the need for preparing for cyber threats has increased. Yet, half of the organizations do not invest in improving cyber security. The study included both public and private organizations from different industries, such as retail, services and transport, banking, energy and water and public administration and defence in Finland. (CGI – – 2016; 1–2, 8.)

Despite the increasing infosec risks, the information security services utilized by companies operating in Finland still remain unclear. Thus, identifying and mapping information security services and understanding their use in companies will help in building both information security knowledge and better information security capabilities in Finland. Furthermore, as the number of information security solutions is growing and new types of services enter the market, it is vital to help organizations better understand what

kind of information security services are available. Additionally, when more information on how to protect themselves against information security threats is available for organizations, it will create more trust towards digital business. Consequently, this thesis aims at tackling these issues and bringing new information and knowledge on the topic in order to encourage the adoption of digital business within organizations in Finland.

The rest of the thesis is organized as follows: The first section discusses research methods, whereas the second section constructs a theoretical background for the study. The third section focuses on the systematic literature review and the fourth, in turn, presents a survey and its results. After the survey, discussion of the whole study will be presented. Finally, the thesis will be concluded in conclusions section.

## 1.2 Research gap and Digiwars programme

### *1.2.1 Research gap*

The introduction section presented some problems related to digitalization and information security. However, these topics also offer numerous opportunities for organizations. In order to promote the digitalization of commercial and industrial life, the Ministry of Transport and Communications – together with the Ministry of Economic Affairs and Employment, industry and commerce – have launched an initiative to create a beneficial operational environment for digital services and new business models (Ministry of Transport and Communications 2015). As a part of this initiative, an information security strategy that promotes trust towards the internet and digital operating methods, will be created. (Ministry of Transport and Communications 2015.) The strategy aims at strengthening the ability to detect and resolve information security discrepancies. Additionally, the strategy aspires to invite critical information security knowledge and companies providing information security services to Finland. (Toimintasuunnitelma – – 2016, 76–77.)

Some of the problems noted in the previous section focused especially on the information security service field. With the vast expansion of the information security business field, the solution offering is also facing rapid growth. To better understand the current information security service field in Finland, it is important to map and categorize the different types of solutions utilized in companies operating in Finland. Additionally, the concept of information security services is lacking a clear definition as different terms are utilized interchangeably to describe these solutions as will be demonstrated in the systematic literature review section (chapter 3). Therefore, a clear categorization and definition of information security services will increase the understanding of this field and serve

as a valuable asset for both further studies and for rooting this know-how in Finland. This thesis aims at clarifying these issues. The thesis will be conducted as a part of a larger programme (Digiwars) carried out by the University of Turku. Furthermore, the client of the thesis is the Finnish Government (later referred to as the 'client'). The Digiwars programme will be further discussed next.

### *1.2.2 Digiwars programme*

As mentioned above, this thesis will be conducted as a part of the Digiwars programme by the Ministry of Transport and Communications and the University of Turku. As the financial potential of digital business is vast and technological innovations grow rapidly, information is needed to promote practices that ensure both privacy and safe use of data (Digiwars – – 2017). The Finnish Government regards it as important that the political actions of the European Union aim to improve the availability and offering of reliable and secure digital commodities in the internal markets. Furthermore, attention needs to be directed to the effects that weaken trust towards the digital operating environment, such as wide-scale privacy breaches occurring in networks. To tackle the issues, the Digiwars programme aims to improve the credibility of digital commodities and business models and to strengthen the market and export of digital services in Finland. (Digiwars – – 2017.)

The Digiwars programme is seminal as it supports the above mentioned initiative of the Ministry of Transport and Communications of the Finnish Government to build a favourable operating environment for digital services and new business models. Therefore, this thesis contributes to the key objectives of digitalization in Finland, focusing on the information security – and especially infosec services – perspective. The next section presents the research questions and describes the study aims and methods in more detail.

## 1.3 The study aims, research questions and scope of the study

The aim of this thesis is to examine information security services and to shed light on these services in Finland.

The thesis includes the following two research questions:

- What are information security services and how they can be categorized?
- What are the information security services that are used in companies of different industries in Finland?

The scope of the study includes the clarification and categorization of the term information security service through a systematic literature review (SLR) and a survey aimed

at investigating the information security services utilized in companies operating in Finland. The systematic literature review follows a qualitative approach, whereas the survey as the empirical part of the thesis employs both qualitative and quantitative characteristics. Therefore, as the study combines both qualitative and quantitative types of research, a mixed methods approach has been chosen. The scope of the study has been defined as part of the larger Digiwars programme based on client needs. The scope of the study in brief consists of:

- information security service term clarification (SLR and survey)
- categorization of infosec services (SLR)
- identification of the infosec services that are used in companies of different industries Finland (survey).

## 1.4 Philosophical background

This section discusses the philosophical stance of the research. Usually this section is handled after the theoretical background but in this study the topic is situated as an introductory theme as it presents the lens through which the whole research will be observed and which guides the execution of the study. Hirsjärvi, Remes and Sajavaara (2003, 117) explain that research is based on numerous latent assumptions on aspects such as human, the world and data collection methods – these assumptions can be defined as the philosophical worldview of research. Similarly, Hakala (2005, 150) states that there are hidden philosophical, methodological and conceptual factors that influence a thesis. These factors form the foundation for the research, whether or not the researcher is aware of them. (Hakala 2005, 150.) Hirsjärvi et al. (2003, 117) note that knowledge on the philosophical assumptions will help in understanding the differences in quantitative and qualitative research. Consequently, the knowledge will help the researcher to explain the logic behind the research decisions he or she has made. (Hirsjärvi et al. 2003, 117.) Therefore, understanding the philosophical stance of the research is important as it affects all the steps of the study from the beginning to the end. This will help in planning and conducting a coherent study.

Some of the key aspects related to the basic philosophical assumptions are ontology and epistemology, which in turn, affect the choices for suitable methodologies and methods for the study. Epistemology and ontology debate about the nature of existence and knowledge (Tieteenfilosofiset suuntaukset 2015). Ontology concentrates on finding out what is reality and what kind of matters are real, whereas epistemology explores the ideas of what kind of knowledge is real knowledge and how and what humans can know about knowledge (cf. Hirsjärvi et al. 2003, 118). The philosophy of science has various orientations from which positivism and interpretivism form the basic division by supporting

opposite ontological and epistemological viewpoints. (Tieteenfilosofiset suuntaukset 2015.) Positivism assumes that a researcher is separate from the environment and the reality he or she is investigating (Weber 2004, 3). Therefore, the reality is formed by facts that can be objectively observed (Hirsjärvi et al. 2003, 129). Due to its nature, positivism is linked to quantitative study (Hirsjärvi et al. 2003, 129) and it concentrates on testing hypotheses and utilizing quantifiable data sources in *generalizing findings* from a sample to a larger population (Orlikowski & Baroudi 1991, 5). Interpretivism, on the other hand, believes that researchers cannot be separated from their reality (Weber 2004, 3) as they interact with their environment, diffuse their own perceptions with it and give meanings to the phenomena related to the environment (Orlikowski & Baroudi 1991, 5). Thus, researchers create *shared interpretations* of their environment and the phenomena related to it (Orlikowski & Baroudi 1991, 5). The interpretivist approach is usually linked to qualitative forms of research.

Additionally, based on the differing worldviews, quantitative research is often seen as a deductive (Inductive Approach – – 2016), top-down approach, where theory is utilized as a basis for hypotheses and their testing, observations and confirmation (Trochim, Donnelly & Arora 2016, 22–23). Qualitative research, on the other hand, is related to an inductive approach (Inductive Approach – – 2016), where the bottom-up process begins with observations, continues with attempts of finding patterns based on the observations and, in the end of the process, proceeds to forming conclusions or new theories (Trochim et al. 2016, 22–23). As this thesis utilizes both quantitative and qualitative methods through mixed methods methodology, it is vital to understand the profound differences in their worldviews. The process of gathering empirical qualitative and quantitative data for the thesis is described in section 1.6.1. Despite the fact that these two differing methods are combined in this study, this research takes the interpretivist stance. Therefore, the basic assumption behind this thesis is that the researcher interacts with their environment and makes interpretations of the environment that influence their findings. This stance is supported by Johnson and Onwuegbuzie (2004, 15–16) who claim a purely objective research of being a myth by noting that despite choosing a positivist worldview, researchers usually belong to some social groups and make subjective decisions during the research process. It could, therefore, be interpreted that the surroundings of researchers influence them and lead them into making subjective decisions. Consequently, some interpretivist influences can even be found from the positivist worldview. In fact, Weber (2004, 8–9) takes the notion further by stating that the discussion on the positivism versus interpretivism paradigm is to a large extent outdated or false and should be ceased. The research premise that demonstrates the basic assumptions of the thesis is capsulized in Table 1.

Table 1 Research premise for the thesis

| Research premise | |
|---|---|
| Philosophical worldview | Interpretivist |
| Methodology | Mixed methods |
| Methods and techniques | Survey with both quantitative and qualitative questions, qualitative systematic literature review |

In conclusion, this thesis adopts an interpretivist worldview and utilizes mixed methods methodology; these choices support each other well and form a coherent basis for the research. The mixed methods approach will be further discussed in the next section.

## 1.5 Research methodology

Various researchers have provided descriptions of a methodology. Van Manen (2016, 27), for example, notes that methodology refers to the philosophical stance or the basic assumptions of research, whereas Creswell and Plano Clark (2007, 4) describe it as "the framework that relates to the entire process of research", which in turn, affects the practices of research (Creswell and Plano Clark 2007, 4). Crotty (1998, 3), on the other hand, describes methodology as the action plan or design that influences the choice of methods and links the methods to the desired results. Methods, then, are the means of conducting the collection and analysis of data (Creswell & Plano Clark 2007, 4). Similarly, Creswell (2003; 6, 13) notes that the researcher merges the knowledge claims or philosophical assumptions to the research design. This implies, that the chosen philosophical viewpoint determines the type of design and methods for the research.

The methodology chosen for this study is mixed methods: As the study combines both quantitative and qualitative elements, it is natural to choose a multi-method approach. According to Creswell and Plano Clark (2007, 5), mixed methods combines quantitative and qualitative data in one or multiple studies. Furthermore, the authors explain that mixed methods can utilize one worldview or adopt multiple worldviews (Creswell & Plano Clark 2007, 5). Additionally, mixed method approach offers multiple advantages. As it combines qualitative and quantitative research, it can offer benefits from both sides (Johnson & Onwuegbuzie 2004, 21, 23). Consequently, as the researcher is not limited to utilizing the methods of a single approach, they can investigate a wider set of research questions. Mixed methods methodology helps in finding more fruitful insights and in compensating the weaknesses of one method with the strengths of the other. (Johnson & Onwuegbuzie 2004, 21.) Therefore, the combination of both data types enables both achieving a more holistic understanding of the research problems examined in the study

(Creswell & Plano Clark 2007, 5) and discovering more evidence for the research findings (Johnson & Onwuegbuzie 2004, 21).

On the other hand, mixed methods methodology also bears some weaknesses as it will require more resources, such as time, money and, sometimes, human resources. Furthermore, researchers utilizing mixed methods will need to understand how to use and combine both methods appropriately. Moreover, researchers that pursue distinct philosophical worldviews, the purists, will not accept the mixing of quantitative and qualitative methods due to their fundamental differences. (Johnson & Onwuegbuzie 2004, 21.) The counter argument to this stance was already presented in the previous section where Johnson and Onwuegbuzie (2004, 15) noted that researchers are surrounded by various social groups and subjective decisions are inevitably made during the research process. Nevertheless, this confrontation that is based on differing worldviews, acts as the basis for the philosophical discussion regarding mixed methods.

Tashakkori and Teddlie (2003) and Greene (2008) (according to Creswell 2010, 10–11) have presented various stances that describe the different views regarding the debate of mixing philosophical frameworks or paradigms in mixed methods. Three of these stances will be presented next based on the notions of Greene (2008, 10–12): According to the first view, the *purist stance*, different paradigms are incompatible and, thus, cannot be combined in a research. The second view named the *complementary strengths stance*, on the other hand, proposes that the paradigms are not inconsistent but differ from each other and, therefore, should be separated in a research. However, it relies on the notion that these differences are valuable in strengthening the research. The third view, the *a-paradigmatic stance*, in turn, relies on the notion that the different paradigms are independent and can be freely combined in various ways in research. (Greene 2008, 10–12.)

When choosing mixed methods, questions on the *primary dimensions* of research design arise (Creswell 2010, 14). According to Greene (2008, 13–14) such dimensions include interaction, status and timing. *Interaction* refers to which degree the different methods utilized in mixed methods research are designed and implemented independently or interactively. *Status*, on the other hand, refers to whether one methodology is prioritized over the others or whether different methodologies are considered as equal in the study. Furthermore, *timing* determines whether the distinct methods are conducted in parallel or sequentially. (Greene 2008, 13–14.) In this study, quantitative and qualitative research parts are regarded as equal as they both seek to find an answer to specific research questions. On the other hand, the types are combined as they complement each other and contribute to the larger theme of information security services. From a process perspective, this cross sectional study is conducted in sequence as the systematic literature review (SLR) is executed first which is then proceeded by the quantitative survey; the results of the literature review will be utilized in the survey. From an empirical perspective, on the other hand, the study is conducted in parallel as the survey part examines both quantitative

and qualitative questions simultaneously. To understand the relevance of the SLR to this study, it is noteworthy to mention, that instead of being a traditional literature review, the SLR conducted in this study represents a type of concept analysis that does not focus on the output of the articles but on the terminology utilized in them. Final conclusions of the results from both research parts will be done concurrently and presented in *Discussion* (chapter 5). The interconnections between the systematic literature review and the empirical part are described in Figure 1.

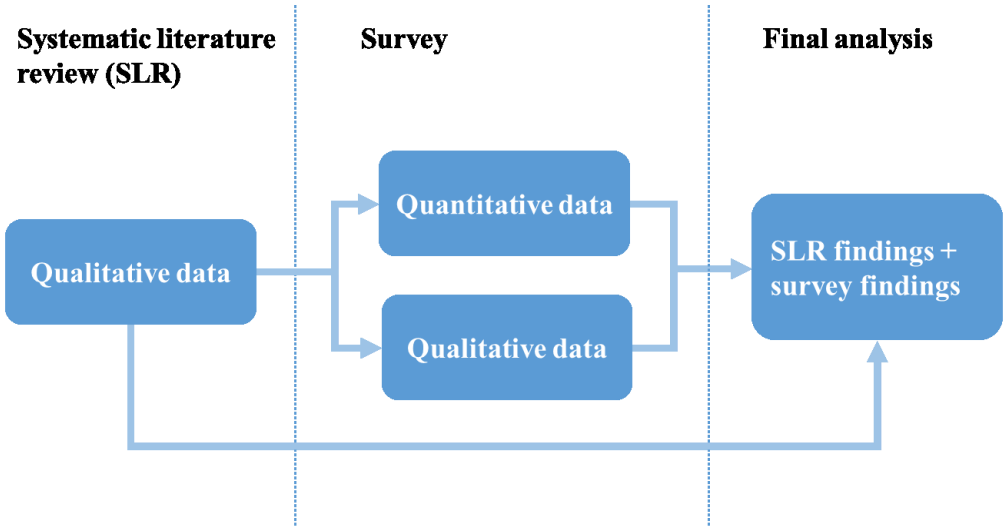



Figure 1 Interconnections between the systematic literature review and the survey

In conclusion it can be stated, that mixed methods as the chosen methodology supports the study aims and research questions well and enables richer results through the mixing of different types of data – qualitative and quantitative. As the study combines different types of research questions, differing approaches and triangulation of different types of data is consequently needed. Utilizing the mixed methods approach in this thesis is further supported as the study combines the survey consisting of quantitative and qualitative elements with a systematic literature review which itself adopts a qualitative perspective. This approach will, therefore, yield best results. Kananen (2008, 11) concludes this idea well by stating that more reliable results can be achieved by utilizing different perspectives. The next section will describe the process for collecting and analysing empirical data in this thesis.

## 1.6 Data collection and analysis methods

From the empirical viewpoint, this thesis process includes a quantitative survey. The survey part aims at complementing the findings of the systematic literature review (SLR) regarding infosec services and identifying the information security services that are used

in companies operating in Finland. Therefore, the survey utilizes the information gained and categorization created in the SLR and elaborates on that knowledge. The following sections describe both the survey data collection and analysis methods utilized in this study.

### *1.6.1 Data collection*

A quantitative research aims at generalizing information from a small group into a population (Kananen 2008, 10). It requires a sample that is both representative and sufficiently large (Heikkilä 2008, 16). Furthermore, quantitative research utilizes numerical information and statistical inference to describe the phenomenon at hand (Heikkilä 2008, 16–17). Qualitative research, on the other hand, utilizes non-numerical information, such as text (Kananen 2008, 11). Furthermore, it aims at understanding the phenomenon through soft information instead of providing statistical generalizations (Heikkilä 2008, 16–17). Although mainly quantitative, the survey in this study also has qualitative characteristics as it includes open-ended questions. The population for this study, in turn, consists of companies operating in Finland. The survey process is described in detail in section 4.1.

The survey will utilize a questionnaire created with Webropol data survey and analysis tool. A good questionnaire is, for example, clear and presentable, the instructions are explicit and the questions proceed in a logical order (Heikkilä, 2008, 48). The questionnaire of the survey consists of both closed-ended and open-ended questions. The closed-ended questions include both multiple-choice questions and a combination of multiple-ended and open-ended questions; an example of such a question would be one that includes the option '*Other, what?*'. Heikkilä (2008, 52) notes that the use of these hybrid questions is useful when it is uncertain if the response options include all possible versions. Another type of closed-ended questions in the questionnaire include scaled questions. These questions utilize five ordered response levels from Likert scale. Likert scale is often utilized in measuring the opinions of the respondent; the scale presents opposite claims at both ends of the scale (Heikkilä 2008, 53). Additionally, the option '*I don't know or do not want to answer*' has been added to separate it from the answer option '*Neither agree nor disagree*' and to give the respondent a possibility to leave the question unanswered. This is supported by Kananen (2008, 24), who notes that to differentiate the unwillingness and inability of the respondent to answer, it should first be clarified whether the respondent can or is willing to answer the question. Furthermore, the lack of the additional option could cause the mixing of neutral opinions, such as '*Neither agree nor disagree*' with the respondent's unwillingness to answer (Kananen 2008, 24). When observing this through the topic of the survey, questions related to the information security issues of organizations can be delicate and, therefore, respondents might feel reluctant to answer them.

Quantitative surveys may include open-ended questions but, opposite to the unlimited questions that utilize associations in qualitative research, they are formed in a way that limit the direction of the respondent's thoughts (Heikkilä 2008, 49). On the positive side, open-ended questions may produce information that cannot be obtained with closed-ended questions (Kananen 2008, 26). However, open-ended questions are laborious to process and categorize (Heikkilä 2008, 49). Moreover, a poorly phrased open-ended question may yield answers that do not benefit the research (Kananen 2008, 25). Furthermore, the respondents may be tempted to leave them unanswered (Heikkilä 2008, 49). This study utilizes open-ended questions as they may bring information that would not be possible to capture with closed-ended questions; therefore it is expected, that the open-ended questions bring more fertile data to certain questions. In general, the survey questions should be clear, necessary for the research, unambiguous, polite and the language used should be correct (Heikkilä 2008, 57). Furthermore, the questions should not be too long, complex or leading and they should address only one topic at a time (Heikkilä 2008, 57.) Therefore, multiple aspects should be taken into account when building a questionnaire. The questionnaire for this survey is available in Appendix 3.2.

According to Heikkilä (2008, 61–62) a survey consists of both a questionnaire and a cover letter. In fact, the cover letter may determine, whether the respondent is willing to answer the questionnaire. Therefore, the cover letter should be polite and inform the respondent of, for example, who is conducting the study, the purpose of the study, how the data of the survey will be utilized and how the respondents for the survey have been chosen. (Heikkilä 2008, 61–62.) These aspects have been taken into consideration in the survey of this study. The next section will discuss the data analysis of the survey.

### *1.6.2 Data analysis*

The data gathered through the survey of this study will be analysed by utilizing both statistical and qualitative methods; the statistical methods will be utilized for the closed-ended questions, whereas the qualitative approach will be utilized for the open-ended questions and for similar options in closed-ended questions. The statistical part will be conducted with Webropol data survey and analysis tool and complemented with analysis. Hypotheses will not be presented in this study as Hirsjärvi et al. (2003, 148) state that hypotheses should be based on theory, theoretical models and prior studies and if such are unavailable, hypotheses should not be utilized. Furthermore, the authors explain that hypotheses are usually utilized in explanatory and comparative studies, whereas in descriptive and exploratory studies not (Hirsjärvi et al. 2003, 148). The latter characteristics better describe this study and, therefore, the exclusion of hypotheses is justified.

The qualitative, open-ended questions will be analysed and, in case of large amounts of data, coded. Yin (2011, 186–187) essentially nominates coding as the *disassembling* of data and describes it as classifying words or parts of the text with codes or labels. Strauss and Corbin (1998, 143), in turn, present various types of coding data, such as selective coding for "integrating and refining the theory", open coding where categories and their characteristics are determined and the differences in the dimensions of those categories examined and, finally, axial coding for systematically developing and linking categories to subcategories. Yin (2011, 186–187), on the other hand, notes that the researcher can also utilize a self-developed method for handling the data. The coding utilized in this study will strive to find main themes or categories within the data.

The findings of the empirical part will be later combined with the findings of the systematic literature review in section 5.1; these will form the final results of this study. The mixing of qualitative and quantitative data will produce better understanding of the research questions (Creswell & Plano Clark 2007, 5) as has been described earlier in this study in section 1.5. The process of combining different datasets was pictured earlier in Figure 1. Next, however, the study will discuss the ethical aspects of research.

## 1.7 Ethical considerations of the research

Ethical aspects are an important topic to be considered throughout the thesis process. This thought is supported by Vilkka (2015, 41), who notes that research ethics – referring to the commonly agreed rules of research – follow the research process from the brainstorming phase through the research results to communication (Vilkka 2015, 41). Responsible conduct of research, which is a topic closely related to research ethics, refers to following ethical research and information sourcing methods accepted by the scientific community (Vilkka 2015, 41). To promote responsible conduct of research, the Finnish Advisory Board on Research Integrity (TENK) (Responsible conduct of research – – 2012, 28–31) has released a guide that presents nine premises for research integrity. Research integrity, according to TENK, refers to the following of ethically responsible and justified modes of operation in research and to the identification and elimination of violations and dishonesty in all fields of research. These principles for the responsible conduct of research state, for example, that research should follow the modes of operation accepted by the scientific community, including integrity, accuracy and meticulousness. Additionally, research should utilize ethically sustainable research, information sourcing and evaluation methods and the publication of results should be done in a responsible and open manner. Furthermore, researchers should appropriately respect the work of other researchers and acknowledge the achievements of others by giving their work proper credit in their own

work. (Responsible conduct of research 2012, 28–31.) This thesis promotes the said principles of ethical research, for example, by following ethical ways of conducting, reporting and evaluating the research throughout the research process and by using proper citations to the work of other researchers.

When discussing the ethical perspective of research, it is useful to consider how reliability and validity can be considered in individual research. Hirsjärvi et al. (2003, 213–214) refers to reliability as the repeatability of research which means that the results of a reliable research should be repeatable by other researchers. Validity, on the other hand, refers to the ability of the chosen research methods in measuring what was intended to be measured. Validity can prove to be a problem, for example, in surveys if the respondents do not understand the survey questions similarly to the researcher. Furthermore, Hirsjärvi et al. (2003, 214–215) note, that even though the concepts of reliability and validity are often linked to quantitative research, the fulfilment of these concepts should be evaluated in all research. In fact, in qualitative research, reliability can be improved by carefully explaining how the research was conducted. The validity of both quantitative and qualitative research, in turn, can be improved by using triangulation. (Hirsjärvi et al. 2003, 214–215.) Denzin (2009, 301–303) divides triangulation into four main types that include methodological, data, investigator and theoretical triangulation. *Methodological triangulation* refers to the triangulation of research methodologies, *data triangulation* refers to mixing various data sources, *theoretical triangulation* refers to using various perspectives and hypotheses when interpreting data and, finally, *investigator triangulation* refers to the use of multiple observers (Denzin 2009, 301–303.) In the latter type, the observers can be interpreted as the researchers of a study.

To increase the validity and reliability of this study, careful descriptions of the steps of the research process, such as of the systematic literature review (SLR), categorization and survey processes, have been included in this thesis. To support these descriptions, in turn, meticulous planning of the phases and reporting of the outcomes of each phase of the research has been done. This is important to ensure coherent, justified and repeatable results from the research. Examples of this are the planning and pre-testing of the survey questions before the survey release, the SLR article inclusion criteria presented in section 3.1 and the inclusion of detailed lists of the identified and accepted services from the SLR. Furthermore, the validity of the research is increased through methodological and data triangulation as the study combines both quantitative and qualitative research through a mixed methods approach. The fulfilment of the validity and reliability aspects in this study is discussed at the end of the research in section 5.2.

# 2 BACKGROUND

## 2.1 Background aims and methods

The aim of this section is to introduce the basic concepts related to information security and information security services and to provide information to support the research questions presented earlier in this study (section 1.3). This information will operate as an introductory pathway to the systematic literature review (SLR) that examines and analyses information security services through academic research. Additionally, the aim of the literature review is to support the research in overall. Furthermore, the literature review section will be named as background in this thesis to separate it from the systematic literature review; the SLR process and results will be presented later in chapter 3. Next the methods for gathering information for the background will be discussed.

Eriksson and Kovalainen (2008, 11–12) suggest finding key words related to one's own research question which helps in finding synonyms and more sources used by other researchers. The authors propose choosing a strategy for conducting the literature review and introduce two different methods for the review: subject key words and citations based. In the *subject key words* based strategy, key words related to the topic of the research are identified and utilized in the literature search. In the *citations* based strategy, the emphasis is in finding new references from the reference lists of articles and other publications. (Eriksson & Kovalainen 2008, 11–12.) In this thesis, both subject key word and citations based strategies will be utilized as using different methods in the literature search process supports the aim of finding rich information on key literature.

The background section will next present the key concepts related to information security and services; the prior topic will be discussed first.

## 2.2 Information security

### *2.2.1 Characteristics of information security*

As societies are becoming increasingly dependent on information systems and engaging in the continuous use of information, it places increasing demands on information security in protecting vital information under different conditions. Information security, therefore, can be seen as a fundamental factor in enabling operations. (Effective information security 2009, 9.) More precisely, the aim of information security is to safeguard the sustain-

able prosperity and continuity of business and to minimize threats (SFS 2012, 18). Consequently, information security includes the application and management of suitable security mechanisms; taking different threats into consideration is also included in this. (SFS 2012, 18.) It is also important to understand what information security is; therefore, this section discusses the concept of information security.

The information security related ISO/IEC 17799:fi standard by the International Organization for Standardization (ISO) defines information security as the act of maintaining the confidentiality, integrity and availability (CIA triad) of information (SFS 2012, 18, 75). *Confidentiality* denotes that the information stored in an information system is only available to authorized users (Hakala, Vainio & Vuorinen 2006, 4). Confidentiality is usually carried out by access control; users are only given rights to use the systems in the extent necessary for their work. The more critical the information system used is, the more important it is to maintain the integrity of data and the ability to return data from a backup file if unwanted changes in the information occur. (Rousku 2014, 47–48.) User names, passwords and encryption are ways of maintaining confidentiality (Hakala et al. 2006, 4).

*Integrity*, on the other hand, refers to prohibiting uncontrolled changes in information; in an organizational context this means that only those people with the permission to make changes can alter the information with the means assigned by the organization. This information includes data sources, such as personal data, banking systems, taxation and insurance information. This information cannot change uncontrollably and there has to be a possibility to return the information at any circumstances. (Rousku 2014, 49.) Consequently, integrity also refers to the conception that the information contained by an information system is accurate and does not include accidental or intentional errors (Hakala et al. 2006, 4). Integrity can be maintained through different solutions, such as setting restrictions to inserted information and utilizing solutions that detect and fix errors (Hakala et al. 2006, 5).

Finally, *availability* refers to information restored in information systems to be available to users with the response time agreed in service level agreements (Rousku 2014, 50). As the world is becoming increasingly digitalized and adopting a 24/7/365 rhythm, information and services need to be constantly available. (Rousku 2014, 50.) Therefore, information should be obtainable from the system quickly enough and in the right format. Availability can be maintained by ensuring that the hardware utilized by information and communications systems is efficient enough and that the utilized software supports information handling in the system. (Hakala et al. 2006, 4.) Additionally, information handling should be automatized as much as possible (Hakala et al. 2006, 5). It can be stated, that information security seeks to protect these three characteristics of information from both threats and accidents (Effective information security 2009, 9).

An example of information that has to maintain its confidentiality, integrity and availability is customer data. If unwanted changes in the data occur, such as changing bank account information, it may result in economic and reputational losses for the company. Similarly, losing customer data through theft can have devastating effects not just on the company but on the customers also. On the other hand, the information has to be available to authorized users according to predefined rules to ensure fluent customer experience and business. As the use of digital services is increasing, companies should pay more attention to securing their customer data. For this, EU has launched the aforementioned general data protection regulation that places increasing demands on organizations to protect and correctly handle their customer data.

Limiting information security to the three above mentioned three components is challenging and, thus, there are numerous additions to the classic triad definition of information security. Siponen and Oinas-Kukkonen (2007, 62) add another dimension to the information security triad (CIA) – *non-repudiation*. This refers to an individual not being able to deny an action, such as signing a contract, afterwards (Siponen & Oinas-Kukkonen 2007, 62). Therefore, the system should include the ability to reliably recognize and record the information of the user; non-repudiation can be carried out through encryption solutions with time-limited user rights or by utilizing biometric identification, such as fingerprint identification. Non-repudiation supports the identification of both the origins of information and unauthorized use of information. (Hakala et al. 2006, 5.) Hakala et al. (2006, 5) also note that the classical information security triad is seen as insufficient as it neither pays enough attention to the identity of the information provider and owner, nor recognizes the value of hardware and information and communications systems. They present a wider definition for information security that include CIA, non-repudiation and access control. *Access control* refers to restricting the use of information handling infrastructure, such as data-communications connections and hardware for personal purposes as they burden the connections, weaken usability and might subject the company to malware exposure. Another possible feature to include is *authentication*, which refers to the reliable authentication of information system users and equipment. (Hakala et al. 2006, 5–6.) ISO/IEC 17799:2005 standard also recognizes non-repudiation as an important factor and, additionally, proposes *authenticity*, *responsibility* and *reliability* as characteristics of information security (SFS 2012, 75). It is noteworthy to mention that the various definitions are not clearly distinctive but can be regarded as overlapping.

Information security is obtained by implementing security mechanisms that have been chosen through a risk management process and are managed through an information security management system. The information management system includes a policy, processes, procedures, organizational structures, software and hardware, that are utilized to protect information assets. These security mechanisms need to be defined, implemented, managed, reviewed and improved if necessary to guarantee that the security and business

objectives of an organization are met. These information security mechanisms need to be seamlessly integrated with the business processes of an organization (SFS 2012, 18.) Nonetheless, policies and systems do not alone guarantee the security of information. According to ENISA (2006, 8), people are a more important factor in information security than technology. Additionally, employees pose a far higher threat on information security than external intruders. Therefore, information security cannot be viewed merely as a technical issue but a management issue (ENISA 2006, 8) and, similarly to information systems, people possess a key role in it. In conclusion, information security can be described as a chain where the weakest link determines the strength of the whole chain (ENISA 2006, 8). The next section, in turn, will distinguish and discuss some key concepts related to information security.

### *2.2.2 Information security, cyber security or data privacy?*

When discussing information security, the terms cyber security and privacy also emerge. To distinguish the three terms from each other, the latter two terms will be briefly discussed next. As von Solms and van Niekerk (2013, 97) note, information and cyber security are often referred to as synonyms but, in fact, bear differences. According to the authors, information security refers to the protection of information from mischief caused by both vulnerabilities and threats. Information in this concept is regarded as an asset and human aspect as the role of people participating in the infosec process. Cyber security, in turn, extends to safeguarding other assets besides information, and people are not only regarded as vulnerabilities or possible sources of cyber threats but also as the targets of such threats. Thus, people should be regarded as assets that need to be protected. The authors conclude that cyber security, therefore, does not merely refer to safeguarding cyberspace but to protecting any actors and their assets that operate and are accessible in cyberspace. (Von Solms & van Niekerk 2013; 97, 101.) Furthermore, the authors distinguish information and communication technology (ICT) security from the two prior concepts and depict their interrelations in Figure 2 (von Solms & van Niekerk 2013, 101).

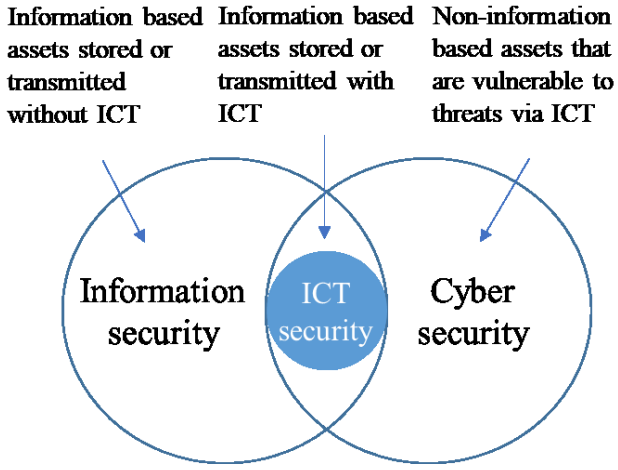



Figure 2 Information, cyber and ICT security (adapted from von Solms & van Niekerk 2013, 101)

The depiction illustrates that information security comprises both information that are handled with information communication technology and with other means, whereas cyber security refers to both information and other assets vulnerable to threats via information and communication technology. Furthermore, ICT security is a component of information security, whereas information security is a component of cyber security (von Solms & van Niekerk 2013, 101); this affirms the intersections between these concepts.

Other authors have also attempted to make a distinction between infosec and cyber security. Similarly to von Solms and van Niekerk (2013), Rousku (2014, 54–56) states that cyber security as a term is much more comprehensive than information security. Where information security refers to the confidentiality, integrity and availability of information, cyber security, in turn, refers to guaranteeing a reliable cyber operating environment and ensuring the appropriate use of that environment. A cyber operating environment, in turn, consists of multiple information systems and is meant for electronic data processing. (Rousku 2014, 56.) Furthermore, cyber security focuses on safeguarding information systems against risks that threaten their operations, especially emphasizing those key environments that are connected to networks and internet (Rousku 2014, 57). The threats targeted at cyber security environments not only consist of threats towards information security, operational continuity and privacy but also include threats that can be caused by non-electronic sources, such as human error or natural disasters. (Rousku 2014, 54–57.)

Tonge, Kasture and Chaudhari (2013, 67–68), in turn, define cyber security as a function that aims at safeguarding information systems, such as databases, networks and applications, and information itself through technological security and suitable processes. Furthermore, it covers the physical protection of "personal information and technology resources", including software and hardware, from unauthorized access. Cyber security

not only comprises the security of IT systems but also of digital networks including critical infrastructures and cyber space within which they operate. However, according to the authors, mere technological measures are not sufficient to protect those information systems and information but a human aspect must be taken into account in the form of education. (Tonge et al. 2013, 67–68.) In conclusion it can be stated, that if a difference between information and cyber security ought to be drawn, cyber security as a concept is considered more comprehensive than information security.

Privacy is another concept often linked to information security. Privacy protection refers to safeguarding the privacy of individuals and other supportive rights when handling personal data (Valtionhallinnon tietoturvasanasto 2008, 105). Privacy protection includes, for example, prohibiting unauthorized access to personal information, maintaining the confidentiality of information and protecting personal data from unauthorized or harmful use. (Valtionhallinnon tietoturvasanasto 2008, 105.)

Smith, Dinev and Xu (2011, 990–991), in turn, differentiate information, physical and general privacy: *Information privacy* refers to access to identifiable personal information, whereas *physical privacy* refers to physical access either to an individual or to their personal space. *General privacy*, then, comprises the two types. The authors note that the difference between information and physical privacy is rarely pronounced in either research or public discussion; however, they interpret information privacy as *privacy* in their study. (Smith et al. 2011, 990–91.)

Even though privacy is not the main topic of this thesis, it is important to recognize that the new general data protection regulation (GDPR) will compel companies to pay more attention to and invest in their information security. Therefore, understanding the influence of the new regulation on companies is important in this thesis: Investing in information security will most likely result in increased investments in information security products, solutions and services.

## 2.3 Aspects on information security

There are various types of information security and ways of categorizing the concept; this section observes some of these categorizations.

The Finnish Ministry of Finance has set a management group for the digital security of the public administration – VAHTI – that operates as the cooperation, preparation and coordination body for the organizations responsible for the development and control of the digital security of the public administration (VAHTI-toiminta 2017). As part of their operations, the Ministry of Finance and VAHTI have released VAHTI instructions. VAHTI instructions divide information security into the following eight information security areas (Classification of instructions 2017):

- physical security
- administrative information security
- personnel security
- operations security
- equipment security
- software security
- information material security
- data-communications security.

Similarly to VAHTI instructions, Hakala et al. (2006, 10–12) present the same information security areas but distinguish operations security as an area that is embedded in all of the other areas. All of the eight information security areas will be presented in more detail next.

The first three areas handle personnel, physical and administrative information security. The first area, *administrative information security* seeks to guarantee the development and management of information security in an organization (Hakala et al. 2006, 10) by utilizing administrative measures, such as organizational arrangements, specifications of tasks and responsibilities, guidance, training and supervision of staff (Valtionhallinnon tietoturvasanasto 2008, 31). It includes communication with both the parties responsible for security within the organization and with external authorities. Additionally, administrative information security evaluates the impact of law and different contracts to the information security practices of the organization. (Hakala et al. 2006, 10–11.) The second area, *physical security*, on the other hand, includes the protection of – for example – people, premises, equipment and materials (Valtionhallinnon tietoturvasanasto 2008, 30) against both physical threats, such as mischief and burglaries, and environmental threats, such as malfunctions in the heating system and damages caused by fire or water (Hakala et al. 2006, 11). Physical security includes measures, such as guarding and physical access control (Valtionhallinnon tietoturvasanasto 2008, 30). A clear example of this type of security would be electronic locks and key tags. The third area, *personnel security*, refers to managing security factors related to, for example, personnel reliability and suitability, substitution arrangements and personnel protection (Valtionhallinnon tietoturvasanasto 2008, 33). It seeks to guarantee the performance of information system users and limit their access rights to organizational information and information systems. It utilizes methods, such as information system related training, defining rights and responsibilities regarding information systems and checking employee criminal records. (Hakala et al. 2006, 11.)

The next areas handle information material, software and equipment security. The fourth area, *information material security* or data security, refers to measures to maintain the confidentiality, integrity and availability of documents, files and other information

materials (Valtionhallinnon tietoturvasanasto 2008, 101). Furthermore, information material security includes cataloguing, categorizing (Valtionhallinnon tietoturvasanasto 2008, 101), storing, verifying, restoring and destroying information material (Hakala et al. 2006, 11). The fifth area, *software security*, in turn, includes software-related security measures, such as identification, observation, logging and quality control measures (Valtionhallinnon tietoturvasanasto 2008, 68). Other related activities include software testing to ensure the suitability of applications for their planned use, the reciprocal compatibility of software and the reliability and faultlessness of operations. Furthermore, software security includes software version and licence management. (Hakala et al. 2006, 11–12.) The sixth area, *equipment security* or hardware security, on the other hand, refers to activities related to computers and other equipment that are connected to the information systems of an organization (Hakala et al. 2006, 12). Equipment security consists of activities that ensure the usability, operation, maintenance and availability of equipment (Valtionhallinnon tietoturvasanasto 2008, 57). These activities include, for example, testing, maintenance and preparation for equipment ageing (Hakala et al. 2006, 12). Furthermore, equipment security is utilized for ensuring the lifespan of equipment with the help of measures, such as installation, guarantee, maintenance, support services, contracts and safe omission of equipment at the end of its lifespan (Valtionhallinnon tietoturvasanasto 2008, 57). In addition, tasks related to evaluating and minimizing risks derived from the use of equipment, such as the risk of injuries, are included in equipment security (Hakala et al. 2006, 12).

The last two areas include data-communications and operations security. The seventh area, *data-communications security* or telecommunications security, includes the protection of communication solutions, such as local area networks and other communication systems (Hakala et al. 2006, 12). The area includes safety measures to ensure, for example, the usability of data transfer connections, the protection and encryption of data transfer and user identification; additionally, it includes laws, norms and actions that strive to achieve data-communications security (Valtionhallinnon tietoturvasanasto 2008, 103). Finally, *operations security* includes preparing for risks derived from system usage (Hakala et al. 2006, 12). It includes measures related to the use of IT, the operating environment, data processing and its continuity; furthermore, other measures include support, development and maintenance activities in order to improve information security (Valtionhallinnon tietoturvakäsitteistö 2003, 22).

Hakala et al. (2006, 12) conclude that the division between different information security areas can be seen as artificial as all the areas influence each other and share common factors. However, the division, in addition to the three main components of information security discussed earlier, helps in planning organizational information security. (Hakala et al. 2006, 12.) In fact, identifying the different areas of information security

enables organizations to understand that instead of homogenous information security, there are various types of it.

Whitman and Mattord (2012, 8), on the other hand, presented a more compressed version of the information security areas. These six information security layers are:

- physical security
- operations security
- personnel security
- communications security
- network security
- information security.

Similarly to the previous examples, Whitman and Mattord (2012, 8) define the security layers as safeguarding physical areas from unauthorized access (physical security), protecting people authorized to access the organization (personnel security), ensuring operations and activities (operations security), securing content and media (communications security), shielding networks, their contents and connections (network security) and, finally, ensuring the CIA properties of information assets via awareness building, technology and policies (information security).

ISO 27002 standard (ISO/IEC 27002 2013, 1), on the other hand, discusses information security controls and divides them into 14 categories that are referred to as *security control clauses*; these categories are further divided into 35 main security categories. The 14 security control clause categories (ISO/IEC 27002 2013) have been pictured in Figure 3; the number in front of the name refers to the category number in the standard.

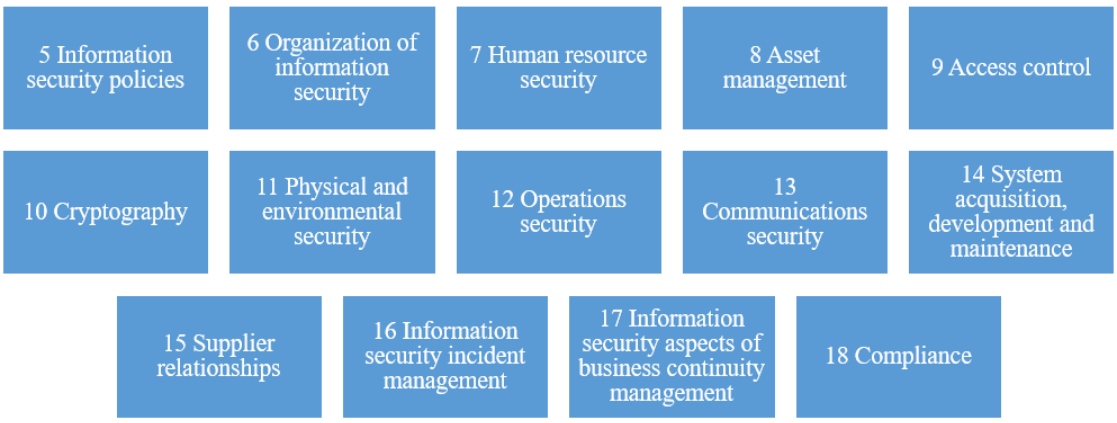



Figure 3 The 14 security control clauses of ISO 27002 standard

The categories address different aspects of information security; each of them will be presented next. The first five categories discuss topics of information security in policies, human resources, asset management and access control; furthermore, organizing infor-

mation within the organization is examined. *Information security policies (5)* concentrates on the management perspective and policies to promote and direct information security within the organization (ISO/IEC 27002 2013, 2). *Organization of information security (6)* proceeds with the management approach and focuses on constituting a management framework for the implementation, operation and control of information security within the organization. This area includes tasks, such as setting roles and responsibilities regarding information security, maintaining relationships with stakeholder groups, such as authorities, and determining policies and security controls for telework and mobile devices. *Human resource security (7)* extends the roles and responsibilities viewpoint and presents measures to be taken into account with both suppliers and employees before, during and after an employment. *Asset management (8)*, on the other hand, discusses the identification and safeguarding of assets within the organization. It consists of defining responsibilities for assets, classification of information and handling of media. The next information security control clause, *Access control (9)*, focuses on controlling access to the information of an organization through business requirements, user responsibilities and user access management. Additionally, this area takes into consideration access control to applications and systems. (ISO/IEC 27002 2013, 2–28.)

The next five categories address the security of operations, communications and physical environment. In addition, cryptography and secure system development is discussed. From the aforementioned areas, *Cryptography (10)* aims to guarantee the suitable use of cryptography in information security and provides guidance on the implementation of cryptographic controls. *Physical and environmental security (11)*, on the other hand, adopts a physical perspective and discusses the protection of the facilities and equipment of an organization. *Operations security (12)*, in turn, observes information security from the perspective of securing the information and information processing facilities of an organization with the help of operational procedures, backups and audits. Additionally, the category discusses event monitoring and logging, technical vulnerability management and protecting the information processing facilities of the organization from malware. The next security control clause, *Communications security (13)*, concentrates on safeguarding information and information transfers within networks and securing the facilities processing the information, whereas *System acquisition, development and maintenance (14)* aims to guarantee information security in information systems throughout their lifespan. The category discusses topics, such as security requirements for the systems, protection of test data and security aspect considerations during the development of information systems. (ISO/IEC 27002 2013, 28–62.)

The last four categories concentrate on business continuity, compliance, incident management and supplier relationships. The latter (*15 supplier relationships*) aims to safeguard the assets of an organization from its suppliers and maintain an appropriate level of security in service deliveries; the suggested means include policies, agreements and

both supplier monitoring and auditing. *Information security incident management (16),* on the other hand, aims to secure efficient management of security incidents with the help of methods, such as defining responsibilities and procedures, reporting and assessing weaknesses, learning form incidents and collecting evidence. *Information security aspects of business continuity management (17)*, in turn, strives to incorporate information security continuity into the business continuity management systems of an organization and suggest redundancies to guarantee that the information processing facilities of the organization fulfil their availability requirements. Finally, *Compliance (18)* refers to securing an organization of any legal or contractual violations related to information security or its requirements; such requirements include, for example, intellectual property rights and privacy. Additionally, the category includes information security reviews to guarantee the compliance of information security operations to the policies and procedures of the organization. (ISO/IEC 27002 2013, 62–78.)

The above presented examples of aspects on information security demonstrate that various parallel ways of categorizing information security exist. Despite their differences, it can be concluded that the different categorizations all strive to both clarify the concept and present the differences between the different types of information security. This study will next, however, focus on another topic important for this research – services.

## 2.4 Services

In order to understand how information security services can be defined, it is seminal to understand what the basic components behind them – services – are. This section not only discusses how services can be characterized, but also examines what are the different ways of categorizing them.

There are various ways of describing services. Kotler and Keller (2011, 356) define a service as “any act or performance one party can offer to another that is essentially intangible and does not result in the ownership of anything”. Vargo and Lusch (2004, 2), on the other hand, parallel services to “the application of specialized competences" with the help of actions and processes that benefit either the entity itself or another entity. Examples of these specialized competences include skills and knowledge. Yet another definition is presented by Wirtz and Lovelock (2016, 21), who state that services are often time-based economic deeds that are conducted by one entity to another one – these deeds or activities provide desired outcomes to their recipients or objects. Furthermore, instead of regarding services as the transferring of ownership, the authors emphasize characteristics of value exchange through economic activities between the two parties involved. (Wirtz & Lovelock 2016, 21.) Following the notions of Wirtz and Lovelock (2016, 21), Kotler

and Keller (2011, 358) present the four pivotal characteristics of services, which are depicted in Figure 4.


Figure 4 The four distinctive characteristics of services

The first two characteristics are intangibility and inseparability. From these the prior trait, *intangibility*, signifies that services cannot be sensed – in other words seen, felt, smelled, heard or tasted – prior to their purchase (Levitt 1981, 37; Kotler & Keller 2011, 358). Additionally, these services can rarely be experienced or inspected beforehand (Levitt 1981, 37). This is the case with, for example, accommodation or application maintenance services. *Inseparability*, on the other hand, refers to the simultaneous production and consumption of services. The provider of the service plays a major role in the distribution of the service as the party purchasing the service may have preferences regarding the provider. (Kotler & Keller 2011, 359.) For example, a customer might feel reluctant to accept the substitution of a senior doctor or consultant with a junior one.

The last two characteristics of a service are variability and perishability. *Variability* illustrates the varied nature of services (Kotler & Keller 2011, 359). It refers to the fact that the provided service varies based on where, when and to whom it is being provided. Additionally, the service provider will influence the service – one customer service representative might be less willing or able to provide good customer service to the customer than the other. Therefore, services can be described as a subjective experience. To decrease the risks of the variability of services, buyers turn to other buyers for feedback of the service, whereas service providers utilize marketing and service guarantees. The final trait, *perishability*, refers to the service being available only when it is being produced; this means that a service cannot be stored which, in turn, can cause problems to the service provider. (Kotler & Keller 2011, 359–361.) Car repair firms, for example, become crowded with customer orders during spring and autumn when the mandatory tire changing period in Finland occurs. Similarly, Kotler and Keller (2011, 361) name public transportation during rush hours as an example of such a service: The service providers need to be prepared for the peak hours with a larger amount of vehicles than would be needed

in the case of even consumption of transportation services throughout the day. Service providers may utilize various methods to level the peaks in demand, such as reservation systems and off-peak discounts. (Kotler & Keller 2011, 361.)

Additionally, the production of services may be, but is not necessarily, connected with physical products. Kotler and Keller (2011, 356) present various service mix categories, in which the role of services in offering varies from low to high. In *pure tangible good*, the offering consists merely of products, such as toothpaste, whereas in *tangible good with accompanying services*, the product is supplemented with a service. (Kotler & Keller 2011, 356.) An example of the latter would be a new car that includes emergency call services. A *hybrid*, in turn, combines products and services equally, such as restaurant meals that combine food with food preparations and serving (Kotler & Keller 2011, 356) or an ERP system with maintenance services. In *major service with accompanying minor goods and services*, on the other hand, the offering mainly consists of the service but is supplemented with minor products or services, such as a flight ticket is accompanied with refreshments. Finally, in a *pure service*, the offering consists only of the intangible service, such as massage. (Kotler & Keller 2011, 356–357.) Another example of a pure service is virtual training.

In addition to the service mix categories, services differ from each other in various ways. Firstly, they can be people or equipment based (Kotler & Keller 2011, 357). An example of the former would be a haircut in a barbershop, whereas launderettes exemplify the latter. Secondly, services can have different delivery processes (Kotler & Keller 2011, 357), such as offering training services through physical lessons or an eLearning course. Thirdly, services meet different needs, which are either personal or business requirements. Fourthly, the need for the presence of the customer varies. (Kotler & Keller 2011, 357.) If we utilize the prior example of a haircut, a customer needs to be present for the service, whereas in the case of dry cleaning or overnight software updates, customer presence is not needed. Finally, services can de differentiated based on their objectives, such as non-profit and profit, and based on their ownership referring to public or private ownership (Kotler & Keller 2011, 357).

Understanding the basic concepts of services is important when moving on to the systematic literature review (SLR) that focuses on the services topic from the information security perspective. The SLR process will be presented next.

# 3 SYSTEMATIC LITERATURE REVIEW

## 3.1 Systematic literature review process

Kitchenham and Charters (2007, 3) explain that a systematic literature review (SLR) refers to a method where a certain research topic is examined through identifying and interpreting all information related to that topic. Systematic literature reviews can be utilized to summarize evidence, to identify gaps in literature or to build a base for new research. The method follows a predefined search plan; therefore, it should present both material that supports the researcher's research question and material that does not support it. (Kitchenham & Charters 2007, 3.)

The benefits of SLR include impartiality and a wide perspective on the research question as the review may include materials that utilize different research methods. On the other hand, systematic literature reviews are more laborious than traditional literature reviews. (Kitchenham & Charters 2007, 4.) This method was chosen for this study as it supported the aim of the research. With the help of SLR, it is possible to handle a wide set of material from which the most suitable articles are chosen for the research.

Kitchenham and Charters (2007, 6) suggest dividing the review process into three phases. These three main phases are planning, conducting and reporting the review which will be referred to as planning, implementation and reporting phases in this study. Each phase includes several steps. (Kitchenham & Charters 2007, 6). The *planning* phase consists of steps, such as identifying the need for a systematic literature review, defining research questions and building a review protocol. (Kitchenham & Charters 2007, 6). A review protocol states the methods chosen for the literature review (Kitchenham & Charters 2007, 12). Additionally, it defines the background for the review, the research questions examined, strategy, criteria and practices for selecting studies, how the quality of studies will be assessed, timetable and strategy and synthesis for data extraction (Kitchenham & Charters 2007, 13). The second phase, *implementation*, consists of steps, such as the selection of initial studies and data collection. The third phase, *reporting*, includes, for example, creating and evaluating the review report. Many steps of the review are iterative as many activities are launched in the planning phase but refined in the implementation phase. (Kitchenham & Charters 2007, 6.) In this study, the review report refers to the SLR analysis and findings sections of the research. The systematic literature review executed in this study follows the three phases previously described. Additionally, the phases have been further divided into seven steps. The whole SLR process is pictured in Figure 5 and presented in more detail next.


Figure 5 Systematic literature review process (cf. Kitchenham & Charters 2007, 6)

The first step of the SLR included the groundwork for the review and creating the review protocol which included, for example, the search terms and article databases to be used. The need for the SLR, background and research questions for the SLR have been presented earlier in *Introduction* (chapter 1). In the second step, in turn, the selection of article databases and search terms was finalized and an initial search was conducted. The chosen article databases included:

- IEEE
- Elsevier ScienceDirect
- Emerald Insight
- ACM – Association for Computing Machinery
- Proquest
- SpringerLink.

These databases were chosen as they are among the most well-known databases in the information systems science research field. The initial idea was to utilise Google Scholar in the search but it soon became evident that, due to practical reasons, it would be better to use the article databases directly as they enable the transfer of material to a reference management software. Therefore, Google was used as a tool for an initial search when

testing search terms. Regarding the reference management software, EndNote was utilized in the first phases of the systematic literature review but this was replaced with Mendeley as it provided better possibilities to handle the documents and make notes and markings during the literature exploration phase. The article search was conducted through advanced search where the search was limited to include journals, scholarly journals, conference papers and proceedings and, in some cases, books. If the books were among the journal search results, they were included in the search but if they were given as a separate list, they were excluded as books were not the main focus point of this research. Only the material that was accessible, was included in the review. The search material will later be addressed as articles in this thesis. The chosen search terms were:

- information security service(s)
- infosec service(s)
- infosecurity service(s)
- IS security service(s)
- IT security service(s).

The terms were chosen based on information security related terms found in literature. To amplify the spectrum of search results, both singular and plural forms of the terms were utilized simultaneously with the help of the search term 'OR'. Quotation marks, on the other hand, were utilized around the terms to limit the amount of irrelevant search results. The initial idea of the study was to utilize the term 'commodity' instead of 'service' but as the initial search with the term conducted in Google did not provide acceptable search results, the term was replaced. These search results were supported with identical results from IEEE, Emerald Insight and Elsevier ScienceDirect databases. After the literature search, all search results were included and transferred to EndNote into separate folders based on article database and search term. The total number of articles at this point was 656. The article search was conducted 4.9.2016.

In the third step, only articles that fulfilled selection criteria were chosen for the next phase. The inclusion criteria required that the term was in some form included in either the title, abstract or key words of the article. The main purpose of the selection criteria was to ensure validity by helping the research focus on the most relevant articles. The number of articles, that fulfilled the selection criteria, was 60. Most of the articles in step two were collected from ScienceDirect and IEEE databases (226 and 167 articles). However, in the third step, most of the articles that fulfilled the inclusion criteria were collected from IEEE (35 articles). In addition to the selected articles, all articles were browsed through to separate those articles that did discuss the topic but did not fulfil the selection criteria. These articles were saved in case the literature review would not otherwise yield a sufficient amount of results. The amount of these additional articles was 141. The division of articles per database in steps two and three is presented in Table 2.

Table 2 Amount of articles per database (SLR steps 2 and 3)

| Step | IEEE | Science-Direct | ACM | Emerald Insight | Proquest | Springer Link | In total |
|---|---|---|---|---|---|---|---|
| **Step 2** | 167 | 226 | 3 | 20 | 121 | 119 | **656** |
| **%** | 25.5% | 34.5% | 0.5% | 3.0% | 18.4% | 18.1% | **100.0%** |
| **Step 3** | 35 | 5 | 1 | 2 | 12 | 5 | **60** |
| **%** | 58.3% | 8.3% | 1.7% | 3.3% | 20.0% | 8.3% | **100.0%** |

In the fourth step of the SLR, the findings were transferred to Mendeley reference management software for better handling. All the articles included in this step were combined and browsed through. Additionally, various search terms were utilised when searching for suitable content from the articles. In total, the results included nine duplicates which were removed. Additionally, other exclusion criteria included both articles that were written in other languages than English and those that did not address the topic. Furthermore, the quality of the articles was estimated and those of very poor quality, such as ones with such poor linguistic quality that they were difficult to read and mistakes in the interpretations could have been easily made, were omitted from the review. Additionally, due to practical reasons, articles that fulfilled the inclusion criteria but were unavailable or did not contain useful material in the abstract, were excluded at this point. In the fifth step, the chosen articles were examined in more detail and the findings from them were recorded into excel. Additionally, an overview of each article was recorded. The amount of chosen articles in the fifth step was 36. As the amount of search results in the final phase was sufficient, the earlier collected additional articles were not included in the review. However, some of these publications were utilized in the SLR findings section to support the SLR analysis.

The sixth step of the SLR included the analysis of the systematic literature review. Even though the writing of the analysis was conducted after the selection of final articles, it must be noted that the analysis of the articles and collection of findings began already during the first steps of the SLR. In fact, the analysis phase consisted of multiple rounds as more services were identified from the articles. This supports the prior notion of the iterative nature of the review process by Kitchenham and Charters (2007). Similarly, the forming of both the analysis and the findings occurred simultaneously during the process. The seventh and final step of the SLR included writing the results and building a categorization in FreeMind mind mapping software based on the findings from the analysis. This task too adopted an iterative nature. The analysis and findings of the systematic literature review will be presented in the following sections.

## 3.2 Systematic literature review analysis

This section focuses on analysing the findings from the articles qualified into the systematic literature review (SLR). During the SLR, a noteworthy amount of information security services was found. All of the synonyms that appear in the articles are not listed in the analysis text; however, comprehensive summaries of the identified and accepted infosec services have been listed after each section. Furthermore, detailed lists containing all of the accepted services from the SLR are presented in appendices 2.1 and 2.2. The articles have been grouped in the analysis based on similar services or other similar factors presented in the text. These groups discuss, for example, articles that rely on standards, concentrate on outsourced security services or embrace the information security triad (CIA) view on security services. Even though the articles have been divided into these perspectives, it by no means signifies that the positions of the articles are absolute. Instead, during the analysis it can be detected that the articles often include various perspectives, based on which they could be positioned into various groups. However, for reasons of clarity, the presented division of articles has been selected. Next we will present the different perspectives, starting with the CIA stance.

### *3.2.1 Security services through CIA*

A substantial portion of the SLR articles presented information security services as very similar to the definition of information security, from which some abided by the information security triad of confidentiality, integrity and availability (CIA), whereas some presented additions or modifications to this traditional listing.

AbdElnapi, Omara & Omran (2016, 175–176) focus on a cloud security context and list confidentiality, integrity and data integrity, availability, non-repudiation and authorization as information security services. According to them, confidentiality strives to prohibit the illicit distribution of data, whereas integrity is important in a cloud storage environment as it helps to safeguard information from illicit actions, such as content changes or removal. They continue by noting that digital signature can be utilized to maintain data integrity. Availability, on the other hand, refers to the availability of data, software or cloud storage to authorized users, whereas authorization helps to specify the people allowed to access certain systems and information. Additionally, the authors refer to the article by Zissis and Lekkas (2012, 586) by noting that availability also includes the capability of a system to perform actions despite misbehaviour from authorized users. Finally, the authors describe that non-repudiation refers to the sender of a message not being able to deny sending the message afterwards (Feng, Chen, Ku & Liu 2010, 256), therefore, verifying the sender's signature or message transmission. In addition to being a

method for integrity, digital signature alongside encryption algorithms and hash functions, are described as *techniques* that provide security services. (AbdElnapi et al. 2016, 175–176.) Interestingly, the analysis will later demonstrate that similar solutions have been described as services by other authors such as Xia and Hu (2006), Tamilarasan, Shankarapani, Qin, Mukkamala and Sung (2008) and Lin and Zhixin (2010). Nevertheless, these terms will not be included in the categorization from AbdElnapi et al. (2016).

Miguel, Caballé, Xhafa and Snasel (2015) take a stance similar to AbdElnapi et al. (2016) concerning information security services by naming CIA as infosec services. The authors (Miguel et al. 2015, 490–492) concentrate on information security services and properties in an eLearning context and describe confidentiality and access control as information security services that both limit students' access rights only to those e-assessment results that have been addressed to them and guide tutors to access the e-assessment information through predefined processes. Additional services mentioned include availability, integrity, non-repudiation, time stamping, authentication, identification, failure control and audit. According to them, availability refers to both the student and the tutor being able to access the e-assessment and integrity, on the other hand, refers to inhibiting any unintentional or unauthorized modifications to the description of an e-assessment. Furthermore, the authors note that integrity should be regarded as both data integrity and authorship. To support non-repudiation, which they refer to as protection against untruthful denial of involvement, the authors suggest time stamping that showcases the existence of the data prior to a specific time. Authentication and identification, in turn, are important services in confirming the identity of the student performing a given task to be assessed and in making sure that the outcome and task at hand match. Audit service, on the other hand, supports e-assessment accountability by registering the evaluation process, whereas failure control safeguards e-assessment against vulnerabilities and negative effects by supplying recovery for the evaluation process in cases of disruptions. Furthermore, the authors note that information security has evolved from singular security methods to *multifaceted solutions*; examples of these include public key infrastructure (PKI), biometric models and solutions that combine various fields of research. (Miguel et al. 2015, 490–492). These solutions have been included in the categorization. Data integrity and authorship are regarded as descriptions and are, therefore, excluded from the categorization.

Similarly to AbdElnapi et al. (2016) and Miguel et al. (2015), Lee, Kim and Kim (2006, 852–853) regard the three components of information security – confidentiality, integrity and availability – as information security services but do not provide further descriptions of them. However, the authors focus on peer-to-peer (P2P) function in their article and contrast the CIA services with the vulnerabilities in P2P. Wahab, Bahaweres, Alaydrus, Muhaemin and Sarno (2013, 4–5), on the other hand, mention data confidentiality, data integrity and availability as security services but, similarly to Lee et al. (2006),

the authors do not provide further information on them. Interestingly, the authors also name the listed services as *parameters*.

Rachedi and Benslimane (2016, 1–3) regard security services as important for arising applications in the area of internet of things (IoT) and reinforce the ideas of Lee et al. (2006) and Wahab et al. (2013) by naming confidentiality and integrity as infosec services. Correspondingly to the notion of Miguel et al. (2015), the authors mention that confidentiality secures that information is only distributed to authorized parties. However, instead of availability, the authors raise authentication as a security service. Accordingly, Rachedi and Benslimane (2016, 1–3) amplify this group of security services by listing examples, such as mutual authentication, relayed-nodes authentication and integrity service, end-to-end authentication and integrity service, end-to-end data confidentiality service and data integrity as infosec services. In addition to these, the authors list parameters, such as message authentication code (MAC), MAC length and encryption key that are related to information security services. (Rachedi & Benslimane 2016, 1–3.) Nonetheless, these parameters will not be regarded as information security services in this study because they were not expressed as such.

Chappell, Marlow, Irey IV and O'Donoghue (1999, 218) discuss information security in the naval shipboard platform context and name confidentiality and authentication as services. Although the authors do not emphasize these as information security services, they will be considered as such in the categorization as they have been identified as services by other authors (e.g., Rachedi and Benslimane 2016 and Miguel et al. 2015). Additionally, Chappell et al. (1999, 218) mention IPSEC as both an internet protocol (IP) security service and an IP security protocol from which the latter is described as a technology that can be utilized to provide security services. Thus, IP security service will be regarded as an infosec service in this study.

Asgarnezhad, Nasiri and Sahebhonar (2010; 562, 565), on the other hand, list integrity, authentication, audit, identity, authorization and confidentiality services as IT security services but concentrate on the two latter. They define confidentiality similarly to AbdElnapi et al. (2016) by stating that it safeguards the non-disclosure of sensitive information that is either transferred through networks or located in data storages. Furthermore, confidentiality is often enabled by cryptographic techniques, such as encryption. Authorization, on the other hand, is a service occurring after the authentication of a user; authorization service refers to determining whether either an authorized or unauthorized user will be granted access. (Asgarnezhad et al. 2010, 565.) Encryption, although described as an enabler of other security services, has been accepted into the categorization as it is nominated as a service by other authors and as it can be interpreted as part of the confidentiality service based on the description in the article. Cryptographic techniques have also been accepted into the categorization as encryption is named as an example of them.

Tamilarasan et al. (2008, 2396–2398) discuss security services and objectives which they exemplify with the notions of Potlapally, Ravi, Raghunathan and Jha (2006, 130–131) by confidentiality, integrity, non-repudiation and authentication. The authors see confidentiality as a seminal information security service which preservation is important and define it as a service that ensures the confidentiality of information being transmitted from one party to another. Additionally, confidentiality ensures that the information is only available to the receiver and is protected against third party interceptions. Finally, the authors discuss security protocols and cryptographic algorithms in the security services context, although it remains ambiguous whether they are referred to as information security services. Tamilarasan et al. (2008, 2397–2398) remark that cryptographic algorithms can be utilized in providing security services, such as integrity, non-repudiation and confidentiality of data. Furthermore, these cryptographic algorithms – such as RSA (Rivest-Shamir-Adleman), DES (data encryption standard) and AES (advanced encryption standard) – can be divided into symmetric, asymmetric and hash algorithms. (Tamilarasan et al. 2008, 2396–2398.) Algorithms and security protocols will be regarded as infosec services in this study.

Peiris, Soysa and Palliyaguru (2008, 307–308) observe information security services in an e-governance setting and state that means to provide security services, such as confidentiality, integrity, non-repudiation, authentication and access control must be ensured for transactions between organizations, governmental institutions and citizen. The authors concentrate on non-repudiation and note that the service must meet the following needs: Proof of origin where there has to be an indisputable relation between the creator of a document and the document itself, proof of integrity where the document cannot be subject to changes after submission and, finally, a third party should be able to verify the non-repudiation of the document. Furthermore, non-repudiation assures the integrity and origin of data. The authors present three types of non-repudiation, which include (Peiris et al. 2008, 307–308):

- non-repudiation of origin
- non-repudiation of submission
- non-repudiation of delivery.

The authors describe that the first type refers to verifying the identity of the creator of a document and the integrity of the document itself (Peiris et al. 2008, 307–308), whereas for the second type they adopt the ideas of Zhou and Gollmann (1997, 268) by stating that it refers to verifying to the creator of a document that the document has been released to a delivery agent for distribution. The third type of non-repudiation, in turn, refers to giving assurance that the document reached its intended receiver without endangering the integrity of the message (Burnett & Paine 2001, 297 according to Peiris et al. 2008, 308). Peiris et al. (2008, 308–309) discuss the implementation of digital signatures to information security services – especially non-repudiation – and present two models, Pretty

Good Privacy and Public Key Infrastructure, from which the first one utilizes web of trust, whereas the second one relies on certificate authority. Additionally, the authors describe digital signature as the hash of a document that has been encrypted with the private key of the document creator. (Peiris et al. 2008, 307–309.) Digital signatures have been included in the security service categorization, whereas certificate authority, web of trust and private key have been excluded from it.

Liping and Lei (2011, 232–234), in turn, name both services that support the CIA triad view but also provide a number of other types of security services. The authors list the following security services (Liping & Lei 2011, 233–234):

- message confidentiality
- information integrity
- transaction non-repudiation services
- authentication
- access control
- session privacy
- source of undeniable
- undeniable purpose
- communications
- key recovery
- security.

Furthermore, the authors recognize public key infrastructure (PKI) as a security service but, simultaneously, note that PKI can offer information security services or *needs*, such as integrity, access control, authentication, session privacy, key recovery, communications, security, undeniable purpose and source of undeniable (Liping & Lei 2011, 232, 234). Other services provided by PKI include encryption and digital signature services that include certificates and passwords. The handling of PKI in the article demonstrates the inconsistent use of terms regarding security services in the articles. Finally, applications with digital signatures and transparent data encryption and other security services concerning certificate and key management have been linked to PKI in the article (Liping & Lei 2011, 234). As the description of some of the services – referring to communications, security, source of undeniable and undeniable purpose – remains vague, they have been left out of the categorization.

Correspondingly to the notions of other authors (e.g., Liping & Lei 2011, Peiris et al. 2008 and Miguel et al. 2015) in promoting access control as an infosec service, Jeong, Joo and Jeong (2010, 3) link access control methods with information security services. The authors also mention dynamic and mobile security services but do not provide clear descriptions on them; therefore, due to their generic nature, these two services have been left out of the categorization.

Some of the articles in this group adopted the CIA triad view, whereas some presented a divergent approach to the traditional approach by proposing alternative or additional infosec services. Examples of such services include authentication and access control. All of the accepted services from the CIA section have been listed below in Table 3; the table presents the pure CIA services and other services including CIA modifications by article.

Table 3 CIA perspective: Identified infosec services

| Authors | CIA services | Other services |
|---|---|---|
| AbdElnapi et al. (2016) | Availability, confidentiality, integrity | Authorization, data integrity, non-repudiation |
| Asgarnezhad et al. (2010) | Confidentiality, confidentiality service(s), integrity services | Audit services, authentication, authentication services, authorization, authorization service(s), cryptographic techniques, encryption (cryptographic technique), identity services |
| Chappell et al. (1999) | Confidentiality | Authentication, IP security (IPSEC) services, IPSEC service |
| Jeong et al. (2010) | - | Access control (method) |
| Lee et al. (2006) | Availability, confidentiality, integrity | - |
| Liping & Lei (2011) | Integrity | Access control, applications with digital signatures, applications with transparent data encryption, authentication, certificates, digital signature services, encryption services, information integrity, key recovery, message confidentiality, passwords, PKI, public key infrastructure, PKI security services, security services to certificate management, security services to key management, session privacy, transaction non-repudiation services |
| Miguel et al. (2015) | Availability, confidentiality, integrity | Access control, audit service, authentication, biometric models (solution), failure control, non-repudiation, identification, public key infrastructures (solution), time stamping<br><br>**Descriptions:** Holistic models, multidisciplinary approaches to security solutions (solution) |
| Peiris et al. (2008) | Confidentiality, integrity | Access control, authentication, digital signatures (for security services), non-repudiation, non-repudiation of delivery, non-repudiation of origin, non-repudiation of submission |
| Rachedi & Benslimane (2016) | Confidentiality, confidentiality service, integrity | Authentication, end-to-end authentication and integrity service, end-to-end data confidentiality, data integrity, mutual authentication, relayed nodes authentication and integrity service |
| Tamilarasan et al. (2008) | Confidentiality, integrity | Authentication, non-repudiation, security protocols<br>AES algorithm, cryptographic algorithms, DES algorithm, RSA algorithm<br>Asymmetric algorithm(s), hash algorithm(s), symmetric algorithm(s) (types of algorithms) |
| Wahab et al. (2013) | Availability | Data confidentiality, data integrity |

The use of CIA as services and its additions and modifications demonstrate that the field of security services is rather scattered. The next group focuses on the use of international standards in defining security services.

### *3.2.2 Information security standards as a basis for security services*

Another approach into defining security services included the adoption of information security related standards; these include especially the standards by the International Organization for Standardization (ISO).

Claassen, Kühn and Penzhorn (1992, 35) utilize ISO 7498-2 standard in describing information security services. The authors mention confidentiality, integrity, authentication, non-repudiation, access control and security audit as security services (ISO 7498-2 standard (1987) according to Claassen et al. 1992, 35). Furthermore, they utilize OSI Basic Reference Model from the ISO 7498 standard and mention that the security services can be placed on different layers of the model but the location influences the meaning of the service. As an example the authors mention, that authentication can be seen as either user, process or host authentication depending on the layer. (Claassen et al. 1992, 35.) Claassen et al. (1992, 36) identify the following services in the layers of the model:

- peer entity and data origin authentication
- access control
- connection and connectionless confidentiality
- traffic flow and selective field confidentiality
- connection integrity with and without recovery
- selective field connection integrity
- connectionless integrity and selective field connectionless integrity
- non-repudiation (origin) and non-repudiation (delivery).

Additionally, Claassen et al. (1992, 35) note that ISO 7498 separates information security services from the mechanisms that provide them; as an example they mention encryption.

Similarly to Claassen et al. (1992), Sun and Chen (2008, 199–200) revert to an ISO standard in defining information security services: The authors suggest defining security services based on the ISO/IEC 27002 code of practice and infosec industry best practices. Consequently, the authors suggest utilizing the "information security and risk controlling activities" in the standard as services. As examples of information security services the authors mention privileged ID monitoring, identity activity monitoring, network access control and network change control, directory management, server change control, external connection review and other security services. They also propose a definition for a security service based on the description of a service-oriented service in the ISO27002 standard; according to them, an information security service is an information security software entity (Sun & Chen 2008, 199) that is "well-defined, self-contained, coarse-grained, loosely coupled and does not depend on the context or state of other services" (ISO 27002 standard according to Sun & Chen 2008, 199). Additionally, the authors describe it as a *compilation of technologies* that enable a developer to "publish, discover,

and invoke application logic using ubiquitous and standard web technologies" (Sun & Chen 2008, 199). The service 'other security service' has been left out of the categorization due to its ambiguity.

In this section, the authors identified infosec services through standards, especially focusing on the globally acknowledged ISO standards. All of the services accepted from these articles have been listed in Table 4. The next section, however, focuses on models and frameworks.

Table 4 Infosec services through standards: Identified infosec services

| Authors | Services |
|---|---|
| Claassen et al. (1992) | Access control, audit, security audit<br>Authentication, user authentication, process authentication, host authentication, peer entity authentication, data origin authentication<br>Confidentiality, connection confidentiality, connectionless confidentiality, selective field confidentiality, traffic flow confidentiality<br>Non-repudiation, non-repudiation (origin), non-repudiation (delivery)<br>Integrity, connection integrity with recovery, connection integrity without recovery, selective field connection integrity, connectionless integrity, selective field connectionless integrity |
| Sun & Chen (2008) | Directory management service, external connection review service, ID activity monitoring service, network access control service, network change control service, privileged ID monitoring service, server change control service |

### *3.2.3 Models and frameworks incorporating information security services*

Some of the articles present models or frameworks that are connected to information security services; furthermore, some authors develop and introduce new security services. These articles will be introduced next.

Deng, Bhonsle, Wang and Lazar (1995, 50, 52–53, 60) introduce a distributed security architecture to be implemented into object-oriented distributed computing systems, such as the common object request broker architecture (CORBA). As part of the security architecture, security services are needed to prevent threats, such as masquerade where the identity of an authorized party is adopted and abused, information disclosure where information is given to an unauthorized party and integrity violation where illicit creation, destruction or modification of data jeopardizes the consistence of the data. As examples of such information security services Deng et al. (1995, 52) mention:

- message confidentiality and integrity protections
- client or object authentication
- security audit
- intrusion detection
- object access control.

According to the authors, authentication occurs between a claimant that wishes to be recognized as authentic and a verifier that aims to ensure the authenticity of the claimant. Consequently, authentication helps in verifying the identity of the claimant and provides protection against masquerade. In addition to this, the authors discuss message origin authentication and message authentication, confidentiality and integrity services. Similarly to the previously mentioned authentication, message origin authentication verifies the identity of the client or object of a message, whereas message integrity safeguards the message against unauthorized modifications, replacement or replay. Message confidentiality, on the other hand, refers to the preservation of the message information against any changes or substitutions and distribution to unauthorized parties. Similarly to the notion of Tamilarasan et al. (2008) regarding the provision of services through algorithms, the authors mention that message confidentiality, integrity and authentication are offered through mechanisms, such as digest algorithms (e.g., MD5 message digest algorithm), symmetric and public-key cryptosystems, such as DES and RSA, and timestamps (Deng et al. 1995, 53). Lastly, Deng et al. (1995, 53) describe that access control safeguards against the threats of integrity violation and information disclosure by managing the access rights and activities of a client. The authors divide access controls into mandatory and discretionary, where the former refers to limiting access rights by granting clients certain security levels according to security policy. The latter, on the other hand, limits the requests a client can perform on a server object. (Deng et al. 1995, 53.) As the mechanisms have been regarded as security services by other authors (e.g., various algorithms by Xia & Hu 2006 and Tamilarasan et al. 2008, cryptographic mechanisms by Kovač & Trček 2009 and time stamping by Miguel et al. 2015) they will be regarded as security services in this study.

In their article, Jin, Cho, Choi and Ryou (2003, 793–794, 796–798) also adopt the framework-oriented approach and develop a unified security framework for providing security services. The authors note that in order to manage information security concerns, such as disclosure and misuse of data, appropriate information security services must be in place. As examples of such security services they mention authentication, authorization and audit. The authors highlight the importance of integrating and managing security services to prevent emerging security vulnerabilities and rising administrative costs; these integrated services are named as unified security services or unified management services. As examples of security services tackling new types of threats they list authentication, authorization, identity management and single-sign-on (SSO). The authors also describe services needed for application integration security in more detail: As the paramount service they nominate identity (ID) management and describe it as managing and allocating both personal and identifier information. They link ID management to authentication by proposing a unified authentication and identity management service as they state that the purpose of authentication is to confirm the identity of a user. Authentication,

on the other hand, includes various methods, from which biometric identification is mentioned. The authors note that if ID management and authentication services are integrated, it will enable the user to enter services with a single password and single authentication. Furthermore, the authors continue that multiple processes, such as utilizing authorization information for an access control decision, may together form a single service. SSO, on the other hand, is described as a service that enables single login to an application without a need for multiple logins when entering other applications. Privilege management and access control, in turn, are given as synonyms for the authorization service. Authorization refers to making decisions about granting access to an application based on predefined policy. Authorization decisions become complicated in the case of integrated and complex applications. Additionally, the authors parallel authorization with audit by stating that the former refers to monitoring before executing an action, whereas the latter refers to monitoring after it. Due to this linkage, both services have similar requirements.

In addition to these services, Jin et al. (2003, 798) mention consolidated billing which is referred to as both a service and a security requirement. The authors describe it as a method for providing a tailored and value-added service that enables both unified payments for multiple services at once and reduced payment collection costs. Furthermore, Jin et al. (2003, 796), give examples of services that support unified authentication and identity management – Microsoft Passport service, LibertyAlliance and Security Assertion Mark-up Language (SAML), but at the same time note that these are considered either more as of standards and frameworks or lack some security services, such as anonym and pseudonym for privacy protection. (Jin et al. 2003, 796.)

Keeratiwintakorn and Krishnamurthy (2006, 1–2, 4) observe information security services from an energy consumption perspective and develop a model that combines information security services with energy efficiency. Furthermore, the authors develop an energy efficient information security service. As security services, the authors list encryption service and encryption in pervasive networks, confidentiality and message authentication. However, the authors also state that message authentication and packet encryption are enabled by the developed security service. Additionally, the authors note that instead of a fixed security level, there are varying security levels, such as low, medium and high (Irvine & Levin 2000, 93–94); the authors utilize this idea in the model. (Keeratiwintakorn & Krishnamurthy 2006, 1–2, 4.) Packet encryption alongside message authentication will be regarded as security services in this study.

El Yamany and Capretz (2008, 551–552, 558), in turn, develop a security service for a service oriented architecture (SOA) that utilizes data mining and an intelligent core. According to the authors, a SOA environment consists of various layers, from which one contains information security services. The authors do not describe the services in detail but list authentication, audit and authorization as examples of information security services, from which the authentication service is especially important as it interacts with

the security service developed in the article to both enable the authentication process and to provide protection against security attacks. In addition to information security services, the authors mention *traditional security techniques* and list secure sockets layer (SSL) technology and virtual private networks (VPN) as examples of these methods. These too will be regarded as information security services in this study.

Lu et al. (2015, 42, 47) develop a framework for emergency ocean oil spill command information systems in their article. Similarly to the SOA environment in the article of El Yamany and Capretz (2008), the framework consists of layers, from which one includes information security services. The authors do not immerse in IT security services but mention a few of them as an example; the listed services include identity authentication, access control, intrusion detection and information encryption. After the framework perspective the study will next discuss outsourced information security services.

This section focused on the various models and frameworks through which infosec services were mirrored in the articles; furthermore, the section also noted that some of the authors developed infosec services of their own. The models ranged from energy efficiency to oceanic emergency systems and SOA architectures. This demonstrates that the context of the articles in the SRL varies significantly between the articles, which could affect the types of services presented in the articles. All of the accepted infosec services have been listed in Table 5. After frameworks, the analysis will focus on managed security services.

Table 5 Frameworks perspective: Identified services

| Authors | Framework / model | Services |
|---|---|---|
| Deng et al. (1995) | CORBA (common object request broker architecture) architecture | Access control, access control service, object access control<br>Access controls: Mandatory access control, discretionary access control<br>Authentication, authentication service, client authentication, message authentication services, message origin authentication, object authentication<br>Message confidentiality, message confidentiality protections, message confidentiality services<br>Message integrity, message integrity protections, message integrity services<br>Intrusion detection, security audit<br>Digest algorithms (e.g., MD5) (mechanism to provide services)<br>Public-key cryptosystems (e.g., RSA) (mechanism to provide services)<br>Symmetric cryptosystems (e.g., DES) (mechanism to provide services)<br>Timestamps (mechanism to provide services) |
| El Yamany & Capretz (2008) | SOA (service oriented architecture) | Audit service, authentication service, authorization service<br>Secure sockets layer (SSL) technology (traditional security technique), virtual private networks (traditional security technique) |
| Jin et al. (2003) | UASI (unified application security infrastructure) framework | Access control, audit, anonym (for privacy protection), authentication, authentication service(s), authorization, biometric identification (authentication mechanism), consolidated billing, ID management, identity management, identity management services, privacy protection, privilege management, pseudonym (for privacy protection), single-sign-on (SSO), unified authentication and identity management, unified authentication and identity management service(s), authentication and identity management service |

| | | |
|---|---|---|
| | | **Descriptions:** Unified management service, unified security services |
| Keeratiwintakorn & Krishnamurthy (2006) | TSM (Tunable Security Model | Encryption, encryption in pervasive networks, encryption service, confidentiality, message authentication, message authentication service, packet encryption<br><br>**Descriptions:** Energy efficient security service(s) |
| Lu et al. (2015) | A framework for emergency ocean oil spill command information systems | Access control, identity authentication, information encryption, intrusion detection |

### *3.2.4 Managed security services*

Some of the articles observe information security services through outsourcing as organizations are often interested in outsourcing some or all of their information security services to an external service provider. These articles discussing managed security services will be introduced next.

Karyda, Mitrou and Quirchmayr (2006, 405–407) focus on the outsourcing of information security services theme and present a comprehensive list of managed security services. The authors explain that the concept of managed security services refers to the management of the human and physical resources – that support the security operations of an organization – by an external provider that has expertise in information system and IT security. However, Karyda et al. (2006, 407) continue that despite the increase in the outsourcing of infosec services, services regarded as sensitive ones are likely to be managed within the organization; these services are nominated as in-house security services. Additionally, the authors note that finding a balance between outsourced and in-house security services will enable better management of information security within the organization. Karyda et al. (2006, 407) provide an extensive list of outsourced security services that include:

- security training and education
- user access management
- IT auditing
- network monitoring
- server management
- virus protection and email virus and spam filtering
- firewalls and firewall management and configuration
- management of virtual private networks (VPN)
- intrusion monitoring and management of intrusion detection systems
- security upgrades
- penetration testing
- disaster recovery

- data classification
- security systems management and monitoring
- business continuity planning and contingency planning
- application and development of security policies.

In addition to these infosec services, the authors revert to the article by Allen, Gabbard and May (2003, 3) and name content filtering services, data archiving and restoration, network boundary protection that includes managed services for firewalls and incident management that includes emergency response as information security services that are often outsourced to managed security service providers. Furthermore, the authors name firewalls and VPNs as outsourced "security installations" or functions that offer encryption services. (Karyda et al. 2006, 407.) These too have been recognized as information security services in the categorization.

The article by Oladapo, Zavarsky, Ruhl, Lindskog and Igonor (2009, 456–457, 460) also discusses the outsourcing of information security services. The authors agree with the prior notion of Karyda et al. (2006) by mentioning that although outsourcing security services is increasing, the security services most sensitive to an organization are rarely outsourced – even if outsourcing is supported by organizational policies (Oladapo et al. 2009; 456, 460). Examples of outsourced security services include physical security, access control, audit, intrusion detection, firewall management and configuration management, security awareness and training and media protection. Oladapo et al. (2009, 457) continue by noting that one of the aims of outsourcing is to decrease the risk towards the confidentiality, integrity and availability (CIA) of information and systems. Consequently, maintaining the CIA of information assets is also described as one of the main purposes of information security services. However, outsourcing also bears some risks, such as decreased control on processes, increased dependency issues, compliance regarding laws, implications of sensitive breaches and IT security maturity within the organization. (Oladapo et al. 2009, 456–457.)

Similarly to Karyda et al. (2006) and Oladapo et al. (2009), Choi and Seo (2005, 624–626) also discuss managed security services (MSS) but highlight the importance of network security. The authors recognize an extensive amount of information security services and begin by listing the aforementioned managed security services, such as security maintenance, analysis of security attack events, management support for security equipment and local and remote security control for infrastructure which includes servers, databases and networks. Analysis of security attack incidents, equipment management and operation of security equipment, on the other hand, they refer to as managerial security services. Some services, such as security maintenance and consulting, are characterized to be both. (Choi & Seo 2005, 624–626.) In addition to these services, the authors propose security services that better correspond to the needs of network security; these services

consist of managed VPN that refers to offering a virtual private network, managed firewall that refers to running existing firewalls, managed filtering of web content, managed intrusion detection systems (IDS), managed antivirus and managed scanning that refers to vulnerability analysis (Choi & Seo 2005; 624, 626).

Moulton and Coles (2003, 204–206) continue with the same topic and discuss premium-level managed security services; these services are designed for a limited group of servers in a wide IT infrastructure utilizing highly sensitive information. Monitoring services, intrusion detection and server configuration are named as such services. Additionally, the authors describe that the premium level of security services include server uptime and availability monitoring to detect denial-of-service (DOS) attacks and service disturbances, intrusion detection utilizing network and host-based intrusion detection software, continuous security software updates based on alerts and recommended server configuration for increased security. (Moulton & Coles 2003, 204–206.) These have been recognized as security services in the categorization.

Bahl and Wali (2013, 2014), in turn, combine outsourcing with information security service quality in two of their articles. The first article (Bahl & Wali 2014, 2, 7–8) considers the impacts of information security governance on information security service quality, whereas the second one (Bahl & Wali 2013, 221) surveys the impact of information security service quality to organizational performance. In both of their studies, the authors name the same information security services; these services include network, application, physical and people as required contractually. (Bahl & Wali 2013, 225; 2014, 21.) Although it is cumbersome to understand the idea of people as services, it is worthwhile to understand the role of them in information security. Without the commitment of people in carrying out information security related activities, it is unlikely that all of benefits of those activities could be accomplished. Therefore, people have been included in the categorization as a service. On the other hand, the services provided by Bahl and Wali (2013, 2014) are rather generic in nature and could, therefore, be interpreted as information security classes, such as physical and people related service categories.

The articles in this section discussed infosec services through outsourcing; it can be concluded that, according to the authors, infosec services offer multiple outsourcing possibilities for organizations. However, despite the benefits of outsourcing, it too bears risks and requires a balance with the infosec services produced in-house. The infosec services accepted from the outsourcing articles are listed in Table 6. The next section will focus on technical and non-technical perspectives on infosec services.

Table 6 Outsourcing perspective: Identified infosec services

| Authors | Services |
|---|---|
| Bahl & Wali (2013) | Application, network, people (as required contractually), physical |
| Bahl & Wali (2014) | Application, network, people (as required contractually), physical |
| Choi & Seo (2005) | **Managed security services (MSS):**<br>Analysis of security attack events, managed antivirus, managed filtering, managed filtering (of web content), managed firewall, managed IDS (intrusion detection system), managed scanning, managed scanning (analysis of vulnerability), managed VPN, management support for security equipment, operation of security equipment, security maintenance<br>Remote and local security control for infrastructure such as networks, servers and databases<br><br>**Managerial security services:**<br>Analysis of security attack incidents, equipment management, security consulting<br><br>**Descriptions:** Managed security service(s) (MSS), managerial security services |
| Karyda et al. (2006) | Business continuity planning, content filtering services, contingency planning, data archiving, data classification, data restoration, disaster recovery, email virus filtering, emergency response, encryption services, firewalls, firewall configuration, firewall management, incident management (incl. emergency response), intrusion detection systems management, intrusion monitoring, IT auditing, managed services for firewalls, management of security systems, monitoring of security systems, network boundary protection (incl. managed services for firewalls), network monitoring, penetration testing, security education, security policy application, security policy development, security training, security upgrades, server management, spam filtering, user access management, virus protection, VPN management, VPNs (security installation)<br><br>**Descriptions:** In-house services, managed security services (MSS), outsourced services |
| Moulton & Coles (2003) | Host-based intrusion detection software, intrusion detection, intrusion detection software, monitoring for server uptime & availability (to detect DOS attacks & service disruption), monitoring service(s), network intrusion detection software, security software updates, server configuration, server configuration software<br><br>**Classifications:** Premium level (of) managed security services, premium level security services, premium (level) services |
| Oladapo et al. (2009) | Access control, audit, configuration management, firewall management, intrusion detection, media protection, physical security, security awareness, security training<br><br>**Descriptions:** Sensitive security services |

### *3.2.5 Technical and non-technical perspectives on security services*

Contrary to the intangible CIA triad perspective presented earlier, some authors focus on the technical perspective on information security services that includes mechanisms, such as virtual private networks (VPNs), public key infrastructures (PKIs), algorithms and firewalls. In addition to the articles focusing on the technical perspective, the aspect of non-technical services emerged in the systematic literature review. Both of these perspectives will be introduced next.

Similarly to Bahl and Wali (2013, 2014), Xia and Hu (2006) also discuss information security service quality but relate it to resource reservation protocol (RSVP). The article

does not focus on information security services but presents algorithms as security services. As examples of algorithms the authors mention RSA and DES algorithms. (Xia & Hu 2006, 51–52.)

Lin and Zhixin (2010), discuss public key infrastructures in their article. According to the authors, PKI is a solution that provides information security services by utilizing asymmetric encryption algorithms (Lin & Zhixin 2010, 4). Furthermore, the authors continue that PKI is utilized in areas, such as key exchange, digital signatures and certificate authority (CA) authentication. The infosec services provided by PKI include authentication PKI that helps communicating parties to authenticate each other, perfect key management which is linked to encryption certificate and non-repudiation and integrality. Integrality can be provided by a third party and cannot be disputed by the communicating parties. In contrast to the articles that regard confidentiality, integrity and availability (CIA) as information security services (e.g., Lee et al. 2006, Miguel et al. 2015), availability, integrity, confidentiality, non-repudiation, accountability and controllability are seen as *security problems* concerning e-commerce in this article. (Lin & Zhixin 2010, 4.) Key exchange, digital signature and CA authentication will be regarded as information security services in this study, whereas integrality will not be included in the categorization due to its unclear nature and to the fact that it does not appear in any other article that could give evidence on its content.

Wang, Deng, Lin, Zhang and Yu (2010, 2–3), in turn, name cloud security as an information security service type provided by cloud computing. The authors describe the functionalities of the service that include, for example, the detection of divergent behaviour of software. Furthermore, Wang et al. (2010, 3–5) note that antivirus systems, threat detection and threat detection systems, anti-spam or spam mail filtering which utilizes distributed honeypots, threat perception and sender reputation for spam mail inhibition are based on cloud security; however, they do not clearly indicate whether these are services, solutions or technologies. Meanwhile, Wang et al. (2010, 3) parallel security technologies and services and list the seven paramount technologies or services in cloud security: email, web and file reputation services, automatic feedback service, relative analysis of behaviour service, white list service and data collection service to which feedback contour, honeypot and net crawler technologies are included. In addition to these, the authors mention the following services: intelligent security analysis, intelligent analysis and mining service of security log, distributed power mass data storage, sample data collection which refers to the collection of suspected virus data, threat processing which refers to the handling of collected and analysed virus data and black list service. (Wang et al. 2010, 2–3.) All of the solutions that have been described as being based on cloud security, will be interpreted as information security services in this study. Opposite to other authors (e.g., Choi & Seo 2005), Wang et al. (2010, 5) name VPNs, firewalls, intrusion detection

systems (IDS) and intrusion prevention systems (IPS) as information security *techniques* rather than services. However, these have been included in the service categorization.

Priescu, Patriciu and Nicolaescu (2009, 433), on the other hand, introduce new network security solutions which include decoy services, such as honeypots or decoys that help route attacks away from systems (Bosworth & Kabay 2004 according to Priescu et al. 2009, 433), self-healing tools that help in identifying, assessing and repairing vulnerabilities prior to materializing risks, airgaps that separate trusted networks from the untrusted ones, denial-of-service defences and exit controls. According to the authors, these solutions should be regarded as additional security resources to the more traditional network security arrangements (Priescu et al. 2009, 432–433). Interestingly, the authors refer to these security resources as techniques, services, solutions and tools. Firewalls and encryption, in turn, the authors name as security layers. (Priescu et al. 2009, 432–433.) All of the above mentioned examples will be considered as information security services in this study.

In contrast to the technical security services, the aspect of non-technical security services was also introduced. Chang and Lee (2003, 27–28) concentrate on the Taiwanese information security market and discuss both information security products and services. As security services they list consulting, application and system integration for integrating networks or applications, certification and certification of the internal computer controls of an organization which is connected to standardization; VPNs, firewalls as both hardware and software solutions, intrusion detection, antivirus and antivirus software and encryption, in turn, are referred to as information security related products. Intruder detection, however, is affiliated with security services in the article. Interestingly, the authors name PKI related solutions and security estimation, that helps in identifying errors in a system, as both security services and products. Certificate authority, on the other hand, is linked to public-key encryption and certification-related services in the article. (Chang and Lee 2003, 27–28.) PKI-related security services, public-key encryption and certification-related services will be included in the service categorization. However, it remains unclear whether certificate authority is intended as a security service in the article; thus, it will be excluded from the categorization. It is notable that the solutions categorized as products in this article are seen as services by other authors (e.g., Karyda et al. 2006, Liping & Lei 2011); therefore, they are regarded as information security services from those authors in this study. These findings demonstrate that the division between information security products and services is not clear. Although the discussion on technical and non-technical security services is not highlighted in the text, the division through products and services is noticeable: the services side contains the non-technical solutions, such as consulting and certification, whereas the products side includes more concrete and technical examples of solutions.

This section highlighted the division between technical and non-technical security services; furthermore, it also demonstrated that the technical security services dominate the named infosec services. Additionally, the section pointed out that the division between different terms, such as products and services, is not clear cut. All of the services accepted from this section have been presented in Table 7. The next section will focus on a holistic perspective on information security services.

Table 7 Technical and non-technical perspectives on security services: Identified infosec services

| Authors | Services |
|---|---|
| Chang & Lee (2003) | Application integration services, certification, certification (of the internal computer controls of an organization), certification related services, consulting, intruder detection, PKI-related services, public-key encryption, security estimation, security estimation services, system integration, system integration services (for integrating applications or networks) |
| Lin & Zhixin (2010) | Authentication PKI, CA (certificate authority) authentication, digital signature, key exchange, non-repudiation, perfect key management |
| Priescu et al. (2009) | Air gaps (solution), denial-of-service defences (DOS) (solution), encryption (layer of security), exit controls (solution), firewalls (layer of security), self-healing tools (solution)<br><br>Decoy services: Decoys, honeypots (solutions) |
| Wang et al. (2010) | Anti-spam filtering, automatic feedback service (technology/service), anti-virus system (based on cloud security), black list service, cloud security, data collection service (honeypot, net crawler, feedback contour) (technology/service), distributed honeypots (for spam blocking), distributed power mass data storage service, email reputation service (technology/service), file reputation service (technology/service), firewalls (traditional security technique), IDS (intrusion detection system) (traditional security technique), intelligent analysis service of security log, intelligent mining service of security log, intelligent security analysis service, IPS (intrusion prevention system) (traditional security technique), relative analysis of behaviour service (technology/service), sample data collection service, sender reputation (for spam blocking), spam mail filtering (based on cloud security), threat detection (based on cloud security), threat detection system (based on cloud security), threat perception (for spam blocking), threat processing service, VPN (traditional security technique), web reputation service (technology/service), white list service (technology/service) |
| Xia & Hu (2006) | Algorithms, data encryption standard (DES) algorithm, RSA algorithm |

### *3.2.6 A holistic perspective on security services*

Some articles view information security services from a more comprehensive perspective instead of merely focusing on individual services. Similarly to Miguel et al. (2015), Schultz (1995) and Sidiroglou, Stavrou and Keromytis (2007) discuss information security services from the perspective of providing more holistic services.

Schultz (1995, 13) focuses on firewalls in his article and discusses circuit-level and application firewalls. Schultz labels them as solutions but, at the same time, refers to firewall design and evaluation related consulting as a security service. Schultz's (1995, 13–15) stance on firewalls as solutions or products rather than services supports the ideas of Chang and Lee (2003) but are contrary to the notions of, for example, Karyda et al. (2006)

and Choi and Seo (2005) that recognize firewalls as information security services. In addition, Schultz introduces the idea of a single, ready-to-use "plug-and-play" information security solution (Schultz 1995, 15). This idea could be extended to information security services as well as was proposed by Jin et al. (2003) with the unified security services. Similarly to Chang and Lee (2003), the author inadvertently distinguishes the non-technical security services from the technical security solutions in the article. Nevertheless, as the terminology used in the article refers to firewalls not only as products but also as solutions and as firewalls have been identified as infosec services in other articles (e.g., Karyda et al. 2006, Priescu et al. 2009), they will be regarded as security services from this article as well.

Correspondingly to Schultz (1995), Sidiroglou et al. (2007, 1–2) mention "one-stop shop" information security services provided by managed security service providers. However, they highlight the risks involved as providers lack a holistic enough knowledge on the information security threats. Instead, they propose a modular approach to the provision of information security services that enables flexibility in building the information security capabilities of an organization. To support this idea, the authors develop a model called mediated overlay services (MOSES) that compiles security services. Sidiroglou et al. (2007, 1–2, 6) also list an extensive amount of information security services enabled or supported by the model; these services include:

- antivirus
- worm, email worm and virus detection
- anti-spam and spam detection
- filtering and transparent network-wide filtering
- automated vulnerability detection and mitigation
- distributed intrusion detection systems
- attack inference
- service availability or resilience
- VPN provisioning
- firewall filtering
- worm vaccine that strives to detect and fix software vulnerabilities
- large-scale behaviour analysis of, for example, users or traffic
- WebSOS that helps accessing a web server under a denial-of-service (DOS) attack.

Interestingly, the authors also discuss non-security services that include services, such as software update and backup (Sidiroglou et al. 2007, 6–7). The definition of a non-security service is not stated very clearly in the article but backup is characterized as a service that can offer protection methods against natural and artificial threats. Furthermore, some of the services proposed in the article are also affiliated with products; an example of this is antivirus (Sidiroglou 2007, 2). Other products in the article include

intrusion detection, VPNs, web security, backup, insider misbehaviour detection, firewalls, spam, intrusion prevention, patch management, spam blockers and worm detectors. (Sidiroglou 2007, 2.) Similarly to other authors (e.g., Chang & Lee 2003, Liping & Lei 2011), the article by Sidiroglou et al. (2007) demonstrate the ambiguity in the use of terms. The non-security services, WebSOS and solutions defined only as products have not been included in the categorization. Both the services and the descriptions of services that were accepted from the two articles are presented in Table 8.

Table 8 Holistic perspective: Descriptions

| Authors | Services |
|---|---|
| Schultz (1995) | **Description**: Single plug & play information security solution<br><br>Application firewalls (solutions), circuit level firewalls (solutions), consulting in firewall design, consulting in firewall evaluation, firewalls (solutions, products) |
| Sidiroglou et al. (2007) | **Descriptions:** Modular approach (security services as modules), one-stop shop for security services<br><br>Anti-spam, anti-virus, attack inference, automated vulnerability detection, automated vulnerability mitigation, distributed intrusion detection systems, email worm detection, filtering, firewall filtering, large-scale behaviour analysis (of users, traffic etc.), service availability (resilience), spam detection, transparent network-wide filtering, virus detection, VPN provisioning, worm detection, worm vaccine |

Although the articles did not merely focus on the holistic perspective, they did present the idea of reviewing the big picture and merging together services instead of focusing on individual services. This highlights the fact that organizations should concentrate on developing their security capabilities and services as a whole to ensure seamless integration between the different components of information security. The final section of the SLR analysis focuses on the various infosec service categorizations identified from the literature.

### *3.2.7 Security service classifications*

Some of the articles adopted an overview perspective and provided classifications of information security services. These articles will be discussed in this section.

Datta Ray, Harnoor and Hentea (2010; 276, 279) concentrate on a security risk management theme in a smart power grid context in their article and divide information security services into three categories: prevention, detection and response. Services listed into prevention are authentication, authorization and access control, whereas detection includes services, such as traffic pattern, monitoring and anomalies. Response, on the other hand, includes decision analysis, signature forensics and backup or redundancies for service continuity and restoration. In addition to these IT security services, Datta Ray et al.

(2010, 276) mention confidentiality and availability as seminal security services. Interestingly, they also describe the two latter functionalities alongside integrity and non-repudiation as *security requirements* (Datta Ray et al. 2010, 279) again supporting the controversial use of terms. Integrity and non-repudiation will not be included in the service categorization from Datta Ray et al. (2010).

Interestingly, the division between soft and hard security – that resembles the earlier mentioned division of technical and non-technical security services – emerged as a classification in the articles by Karokola, Kowalski and Yngström (2011a, 2013) and Kovač and Trček (2009). Karokola et al. (2011a, 1–2; 2013, 1792–1793), for example, observe information security services in an e-government context and present a division between technical and socio or non-technical security services. The authors parallel information security services to security aspects and list some examples (Karokola et al. 2011a, 1; 2013, 1794); the technical security aspects include hardware and software solutions, whereas the non-technical ones include awareness programmes, administrative and managerial policies and operational and procedural guidelines, contractual and legal documentation and, finally, cultural and ethical norms (Karokola et al. 2013, 1794). Karokola et al. (2011a, 1) list very similar security services in their earlier study from 2011 but, instead of legal and contractual documents, they discuss frameworks. Additionally, the authors name access control and antivirus mechanisms as examples of software and hardware solutions (Karokola et al. 2011a, 1). Finally, the authors refer to their earlier study (Karokola et al. 2011b, 62) and note, that many of the existing information security maturity models lack the non-technical security services (Karokola et al. 2011a; 1).

Kovač and Trček (2009, 255), in turn, make a division between soft social security mechanisms and traditional hard security mechanisms (Rasmusson & Jansson 1996, 1) and include information security services in the latter. The authors also categorize different information security techniques and mechanisms, such as cryptographic mechanisms and techniques, authentication, access control and authorization – that mainly aim to restrict access rights, safeguard resources and protect confidentiality, integrity and availability of information assets – as hard security mechanisms. Additionally, authentication and authorization are further detailed as access control mechanisms. Soft security – that includes trust and trust and reputation systems – on the other hand, endorses compliance with the rules of the society and penalizes breaches against them. Trust and reputation systems are described as "dynamic rating systems" by the authors and trust is linked to reputation (Kovač & Trček 2009, 256). The description of reputation, on the other hand, is borrowed from Jøsang et al. (2007, 621) who state that reputation is a measure of trustworthiness based on ratings given by the members of a community. (Kovač & Trček 2009, 256). The authors note that hard security mechanisms alone are not sufficient but soft security is needed to safeguard collaborating parties from fraudulent actions, such as

giving false information. (Kovač & Trček 2009, 255.) Even though the authors concentrate on mechanisms and techniques instead of information security services, the article has been included in the analysis as it introduces the softer side of information security and infosec services which is seldom present in the articles, although it enables a more comprehensive perspective on information security and related services. The fact that other authors (e.g., Asgarnezhad et al. 2010, Miguel et al. 2015), have suggested the security measures as services further supports the inclusion of them.

From the article by Vorakulpipat, Siwamogsatham and Kawtrakul (2014) only the abstract is available but, nevertheless, it offers useful insights to the question of information security services. The authors discuss information security as a service in the area of healthcare and suggest combining two different views – a business oriented and an infosec management system (ISMS) view – on information security services. Furthermore, the authors list network services, consulting, software development and helpdesk services as third party provided information security services.

The classifications presented in the above articles demonstrate that information security services can be observed from multiple angles ranging from activities to types of services. Furthermore, these findings strengthen the earlier notions of the versatile nature of infosec services. All of the classifications and services accepted from these articles are presented in Table 9.

Table 9 Identified infosec service classifications

| Authors | Services |
|---|---|
| Datta Ray et al. (2010) | **Classifications:** Detection, prevention, response<br><br>Anomalies, access control, authentication, authorization, availability, backup for service continuity & restoration, confidentiality, decision analysis, monitoring, traffic pattern, redundancies for service continuity & restoration, signature forensics |
| Karokola et al. (2011a) | **Classifications:** Socio / non-technical security services (or aspects), technical security services (or aspects)<br><br>**Socio/non-technical:** Administrative policies, awareness programmes, contractual frameworks, cultural norms, ethical norms, legal frameworks, managerial policies, operational guidelines, procedural guidelines<br><br>**Technical:** Access control mechanism, antivirus mechanism, hardware solutions, software solutions |
| Karokola et al. (2013) | **Classifications:** Socio / non-technical security services (or aspects), technical security services (or aspects)<br><br>**Socio / non-technical:** Administrative policies, awareness programmes, contractual documents, cultural norms, ethical norms, legal documents, managerial policies, operational guidelines, procedural guidelines<br><br>**Technical:** Hardware solutions, software solutions |
| Kovač & Trček (2009) | **Classifications:** Hard security, social control mechanisms, soft security mechanisms, soft social security mechanism, traditional hard security mechanisms, traditional (security) mechanisms<br><br>**Hard security:**<br>Access control (traditional security mechanism), access control techniques, authentication (traditional security mechanism), authentication techniques, authorization, authorization techniques, |

| | |
|---|---|
| | cryptographic protocols (traditional security mechanism), cryptographic mechanisms (traditional security mechanism)<br><br>**Soft security:**<br>Reputation systems (social control mechanism), trust (soft social security mechanism), trust systems (social control mechanism) |
| Vorakulpipat et al. (2014) | **Classifications:** Business-oriented perspective, Information security management system (ISMS) perspective<br><br>Consulting services, helpdesk services, network services, software development services |

The analysis section introduced a breakdown of the articles included into the systematic literature review (SLR). The study will next concentrate on discussing the findings of the SLR based on the analysis. The findings section will first present an overview of the SLR and then examine some of the findings in more detail.

## 3.3 Systematic literature review findings

### *3.3.1 Overview of the systematic literature review*

Before entering into the detailed findings of the systematic literature review, it is useful to obtain an overview of the review and its articles. The SLR consisted of different types of material: mainly conference proceedings (23 papers, 63.9% from articles) but also journal articles and book sections. Table 10 below demonstrates the division of material in the SLR. Both of the articles in the book section category were originally conference proceedings. Additionally, four of the journal articles appeared in magazine-like academic journals.

Table 10 Types of publications in the systematic literature review

| Type of publication | Number of publications | % |
|---|---|---|
| Journal articles | 11 | 30.6% |
| Conference proceedings | 23 | 63.9% |
| Book sections | 2 | 5.5% |
| **In total** | **36** | **100.0%** |

The year of publication for the articles varied extensively from year 1992 to 2016; a compilation of the number of articles based on the year of publication is presented in Figure 6. Interestingly, the largest amounts of publications per year appear between years

2006–2010, whereas one would have assumed that the amount of publications would increase towards the end of the time period considering the current growing interest towards and importance of information security and related topics.

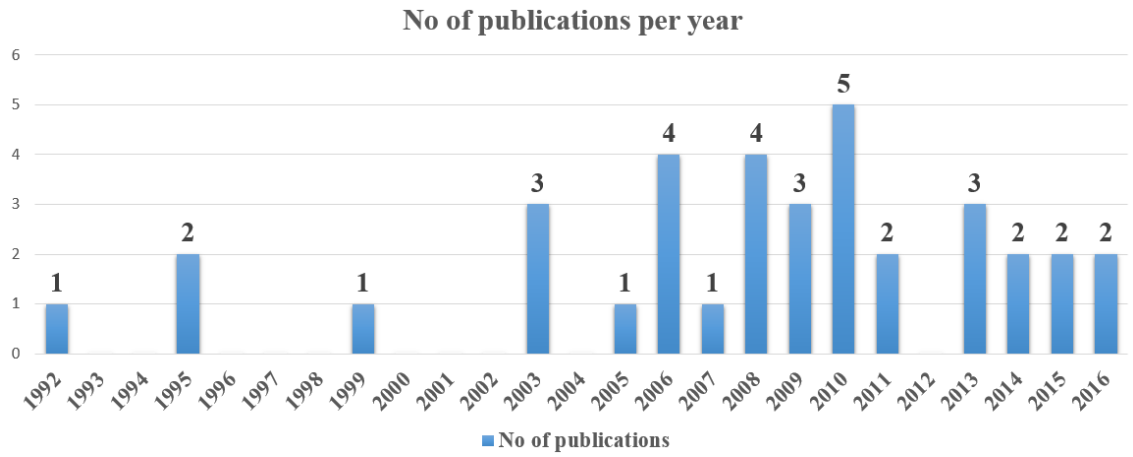



Figure 6 Number of publications per year

Although the amount of selected articles (36 papers) was sufficient for the research, it must be noted that they present only a fraction of the original number of found articles (5.5% out of the 656 articles). Consequently, many of the articles that fulfilled the criteria did not include any description of information security services and, therefore, did not provide any useful content for the research. Additionally, many articles included only very limited lists of information security services without any description of them and some of the given descriptions were somewhat unclear. A few articles were also omitted due to poor quality.

### *3.3.2 Definition of an information security service*

As the analysis demonstrates, the articles in the systematic literature review witness a wide range of information security services. In the analysis section, the articles had been grouped based on similarities in the descriptions and listings of security services. However, before taking a closer look at the services, it is wise to first observe the definition of a security service itself. Interestingly, only few articles included in the systematic literature review (SLR) provide a definition for the term. Sun and Chen (2008, 199) describe information security services as independent software entities and compositions of technologies that are well-defined and both independent but loosely coupled with other services. Oladapo et al. (2009, 457), in turn, note that the prime purpose of security services is the safeguarding of confidentiality, integrity and availability (CIA) of information as-

sets. Kovač and Trček (2009, 255) on the other hand, affiliate infosec services with traditional security mechanisms. One of the definitions provided comes from an additional publication by Buecker et al. (2007, 29), that defines both IT and business security services as parts of a SOA reference model. IT security services are defined as "building blocks to provide security functions as services", whereas business security services are described as utilizing both the IT security services and policy infrastructure in supplying "business specific security capabilities".

Based on these limited findings it can be stated, that many of the articles lacked concrete definitions of what an information security service actually is. This lack of findings evidences the thought that perhaps the definition of a security service is found self-evident and, therefore, only few descriptions were given. On the other hand, it could be, that – based on the spectrum of services identified in the SLR – the concept is seen as too complex and unambiguous to be placed within tight frames. Next we will focus on the different perspectives on security services found during the SLR.

### *3.3.3 Perspectives on information security*

After observing the security service term, we can now turn to look at the groups of services or perspectives that emerged during the SLR in more detail. Some articles discussed outsourced security services, relied on international standards or the CIA triad in defining services, provided classifications of services or observed services through holistic or soft versus hard perspectives, whereas others presented infosec services as part of the authors' own models or developed new security services. Some of these perspectives will be further examined next; the CIA perspective will be discussed first.

The most popular approach in defining information security services was through the three cornerstones of information security: confidentiality, integrity and availability (e.g., AbdElnapi et al. 2016, Lee et al. 2006). In addition to this, descriptions with additions or variations – such as non-repudiation (e.g., Miguel et al. 2015, Claassen et al. 1992), access control (e.g., Deng et al. 1995, Jin et al. 2003), authentication (e.g., Liping & Lei 2011, Datta Ray et al. 2010) and authorization (e.g., El Yamany & Capretz 2008, Asgarnezhad et al. 2010) – to this triad were presented. Defining information security services similarly to information security in general is both an interesting finding and a challenge as the definition remains very superficial and provides little understanding of the difference between these two terms. Perhaps the division can be drawn through scope: information security services are presented as single attributes, whereas information security covers all of the attributes of confidentiality, integrity and availability. It should also be noted that some authors had differing thoughts with the idea of regarding CIA as security services: Datta Ray et al. (2010), for example, referred to confidentiality and availability as

security services but, at the same time, recognized the two alongside integrity and non-repudiation as security requirements. Similarly, Oladapo et al. (2009) supported the stance by stating that the primary purpose of security services is to preserve CIA. These examples showcase how the discussion on what can be considered as a security service is not clear or straightforward.

The standards utilized in the articles included ISO 7498 and ISO 7498-2 (Claassen et al. 1992) and ISO/IEC 27002 (Sun & Chen 2008). Similarly to Claassen et al. (1992), Shaikh, Sharif and Ahmed (2005, 2) revert to ISO 7498-2 in defining security services and list confidentiality, integrity, access control or authorization, authentication and non-repudiation as infosec services. Furthermore, Shaikh et al. (2005, 2) link confidentiality to privacy by stating that the messages delivered should be readable only to the message sender and receiver. Integrity, according to the authors, refers to the data being transmitted to the receiver unchanged, and authentication, on the other hand, signifies that "the receiver is sure of the sender's identity". Shaikh et al. (2005, 2) assimilate authorization with access control and refer it to limiting access rights to resources to concern a particular set of people. In non-repudiation, the authors state, that it is necessary for the receiver to be able to verify that a message came from a certain sender. Additionally, the authors nominate single sign on (SSO) and user provisioning as higher level services provided by security processes. (Shaikh et al. 2005, 2, 6.) The conference paper by Shaikh et al. (2005) did not qualify for the review based on the inclusion criteria but it validates the use of standards in defining information security services.

Another perspective that arose during the review was managed security services which refers to information security services that have been outsourced to a third party (e.g., Karyda et al. 2006, 403). The reasons for outsourcing range from cost reductions to obtaining expertise, improving efficiency and mitigating risks towards information and information system CIA (Oladapo et al. 2009, 456). Although companies are interested in achieving increased security and decreased maintenance costs, they may be reluctant to outsource the services that they regard as highly sensitive to the organization. In addition to outsourcing, the topic of security service quality was present in the articles. Interestingly, only three articles (Bahl & Wali 2013, 2014; Xia & Hu 2006) in the review discussed information security services from the quality perspective. However, information security service quality should be regarded as an important topic as it can affect the overall information security capabilities of an organization.

Many of the articles focused on technical security services overpowering the softer, non-technical approach to information security services. However, the technical security services alone are not sufficient in providing holistic security to an organization. Chang and Lee (2003) and Schultz (1995) made a division between technical products and non-technical services. Karokola et al. (2011a, 2013) and Kovač and Trček (2009), in turn, made an even more visible division between soft and hard security: The prior discussed

technical and non-technical security services, whereas the latter introduced traditional hard security mechanisms and soft social security mechanisms and interpreted security services as traditional hard security mechanisms. Even though Kovač and Trček (2009) discussed mechanisms instead of services, the division between hard and soft security can be applied to infosec services. The softer perspective is especially important as it does not merely promote softer services, such as training and awareness building, but emphasizes the influence of social control and norms of the society in information security: The sole implementation of technical solutions cannot prevent all misbehaviour related to information security but the ideology needs to be implemented into the mindset of the members of the organization or society. Soft services promote this endeavour.

Another interesting finding in the articles was that some authors promoted a more comprehensive perspective on information security services contrary to focusing on individual services. Miguel et al. (2015) described how the field of security solutions has transformed into multidisciplinary and holistic approaches. Schultz (1995, 15) mentioned the desire to obtain a single 'plug-and-play' solution by reason of limited resources, although emphasizing the fact that such a solution would not fit with firewalls due to their need for high maintenance. Sidiroglou et al. (2007), in turn, presented a very similar view with their notion of 'one-stop-shop' security services and by emphasizing the vulnerabilities of the approach if sufficient expertise on security threats is lacking. Instead, the authors presented a modular approach to composing security services that would better serve the needs of an organization (Sidiroglou et al. 2007). Furthermore, Jin et al. (2003) supported the holistic view by promoting the idea of integrating and properly managing implemented security services to counter threats and named authentication and identity service as an example of a unified security service. This perspective demonstrates that focusing on single solutions is not enough to ensure the security of an organization but a more holistic standpoint should be adopted to better serve the overall needs of the organization.

Several classifications were also identified during the systematic literature review (SLR). In addition to the division of soft and hard security provided by Karokola et al. (2011a, 2013) and Kovač and Trček (2009), another classification was introduced by Datta Ray et al. (2010) who divide security services into phases that can be described as information security threat processing steps. Furthermore, two non-scientific publications that presented classifications were found during the SLR process – the first one by Buecker et al. (2007) and the second one by Bowen, Hash and Wilson (2006). Buecker et al. (2007, 28–37, 43–49) discuss business and IT security services and security policy infrastructure as parts of a service-oriented architecture (SOA) reference model of IBM and describe these as the primary elements of security. The business and IT security services listed in the publication are depicted in Figure 7.

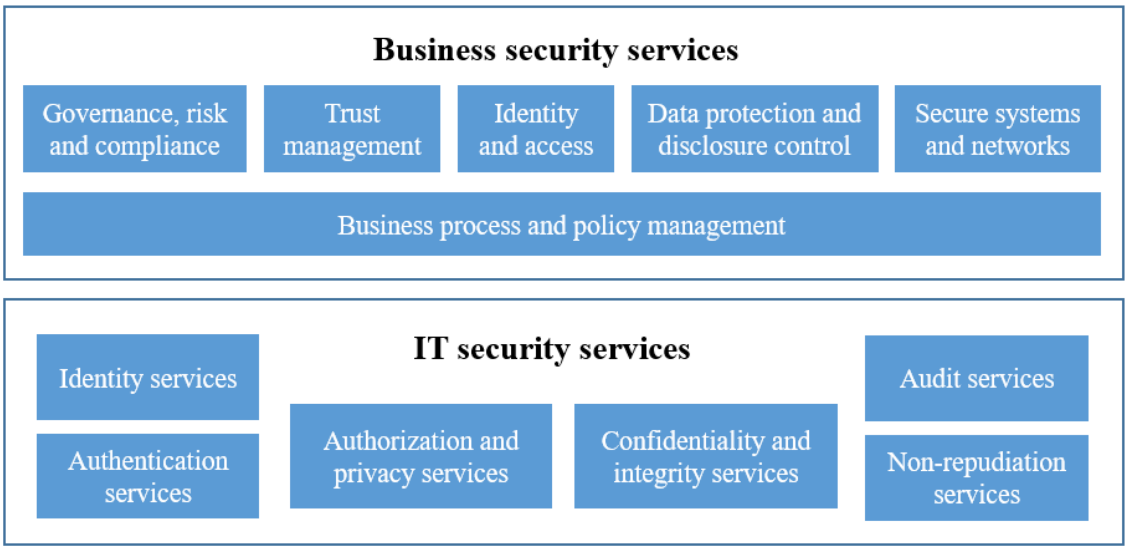



Figure 7 Business and IT security services (adapted from Buecker et al. 2007, 30)

Additional services mentioned in the publication include message and data protection services as subservices to confidentiality and integrity, data and application isolation support services and cryptography as services for data protection, trust service as part of trust management, audit logging services linked to audit services, non-repudiation service for digital certified mail and, finally, authorization services (Buecker et al. 2007, 35–36, 42, 44–46). The division of business and IT security services in the publication supports the earlier mentioned perspective of technical and non-technical security services to some extent.

Interestingly, identity has been listed both as a business and an IT service and policy related components have been separated from the services into a service policy infrastructure entity. The publication does mention operating systems security, firewalls, host and network intrusion detection, patch management and virus detection as part of secure systems and networks security service but refers to these as systems and technologies. (Buecker et al. 2007, 31–32, 38–43, 46–48.) Thus, they have been excluded from the categorization from Buecker et al. (2007).

The second additional publication provided by Bowen et al. (2006, 116), in turn, present three information security service categories, which include management, operational and technical services. Technical services refer to security controls operated by computer systems, whereas management systems refer to the management-led concerns and techniques in a computer security program. Operational services, on the other hand, refer to controls performed by people instead of a system. Interestingly, the authors distinguish information security services from products but do not give clear examples of such products (Bowen et al. 2006, 113–123). The publications by Buecker et al. (2007) and Bowen et al. (2006) emerged during the systematic literature review as additional

material that did not qualify for the SLR; therefore, they were later included in the review as additional articles.

All of the above-mentioned classifications support the previously mentioned holistic perspective as they guide to observe information security services from a wider perspective focusing on larger entities instead of singular measures. In conclusion it can be stated, that the articles introduced various perspectives on information security. Furthermore, the division of perspectives in the analysis section is not clear: In many articles there were elements and security services that were also present in other perspectives. Therefore, many of the articles could have presented various perspectives. Hence, it can be stated that the perspectives presented above are not distinctive but contain overlapping elements.

### *3.3.4 Other findings from the SLR*

This section highlights some observations from the point of view of service types and individual services. The first observation is that the function of an information security service may not be unambiguous. An example of this is certification: Chang and Lee (2003) related the service both to organizational certification and to certificate authority which is a topic existing in cryptography. Similarly, protocols (e.g., security protocols by Tamilarasan et al. 2008, cryptographic protocols by Kovač & Trček 2009) could be linked to management of information security on a higher level or to cryptography on a more detailed level. In the SLR, the protocol-related security services were linked to cryptography based on the contexts presented in the articles. However, this demonstrates that the context bears a significant meaning when interpreting the services. Interestingly, in both of the examples, the prior could be interpreted as a soft service, whereas the second as technical or hard.

In addition to the previous findings, one should also observe the types of security services identified. Most of the services presented were rather concrete, such as firewalls (e.g., Karyda et al. 2006), training (e.g., Oladapo et al. 2009), authentication (e.g., Chappell et al. 1999), intrusion detection systems (e.g., Choi & Seo 2005) or antivirus (e.g., Sidiroglou et al. 2007). Some, on the other hand, had a more abstract nature, such as ethical norms, security awareness or trust. In fact, an interesting finding from the point of view of single information security services is the acknowledgement of trust and trust systems as soft security mechanisms presented by Kovač and Trček (2009). Although trust does not directly seem like a service, the idea is supported by Buecker et al. (2007) who list trust and trust management as business security services. Building and managing trust within an organization can be regarded as a soft security service. On the other hand, trust management includes tangible elements as it includes other more concrete services, such as rating systems. The inclusion of tangible and intangible elements is also visible

in the notion of Buecker et al. (2007, 44–45) who divide trust management into business and technical aspects from which the prior refers to applying agreed rules on making business, whereas the latter refers to cryptographic measures utilized in achieving trust.

The lack of concreteness is especially visible in those services that are also utilized in depicting information security; these services include confidentiality, integrity, availability and non-repudiation. When observing all of these abstract services, the following question emerges: *Can these services be bought?* Perhaps the idea behind these services is that an organization is aiming at obtaining the characteristics by buying the service – a customer is, for example, trying to achieve trust or confidentiality regarding their information assets within the organization. But then again, if these services form the requirements for information security, how do they then differ from the main purpose of information security? The ideology behind naming the abstract characteristics as services remains unclear; however, these measures have been identified as such in multiple articles (e.g., confidentiality by AbdElnapi 2016 and Miguel et al. 2015, integrity by Lee et al. 2006 and Rachedi & Benslimane 2016, security awareness by Oladapo et al. 2009 and norms by Karokola et al. 2011a & 2013).

Other controversial findings include the acknowledgement of people as an information security service by Bahl and Wali (2013, 2014). Perhaps people could be interpreted as enablers or parts of the services, such as consulting, awareness building and education, from the organizational point-of-view due to their importance in implementing the service. Nevertheless, the controversial finding remains somewhat unclear. However, as mentioned earlier, perhaps the services presented by Bahl and Wali (2013, 2014) – especially people and physical – could be regarded as service categories instead.

Physical security itself is another absorbing aspect to be considered as it can be regarded as a contrast to hard and soft security. However, physical security services, such as locked doors, guard services and surveillance, did not emerge on a large scale during the systematic literature review, nor was the topic discussed in detail in the articles, although Oladapo et al. (2009) and Bahl and Wali (2013, 2014) present physical security as a security service. On the other hand, access control – which was present in multiple articles (e.g., Claassen et al. 1992, Lu et al. 2015 and Peiris et al. 2008) – could be understood as a physical security service. Physical security should not be overlooked as it holds an important role in the protection of an organization and all of its assets.

### *3.3.5 About the terminology of the articles*

During the systematic literature review (SLR), it became evident that the articles utilized a myriad of different but overlapping terms, such as services, tools, techniques, solutions, mechanisms, aspects, needs and approaches. Additionally, the form of spelling varied and

often only parts of the search terms were present in the articles; an example of this would be the use of the term ‘security service’ instead of an information security service. This created clear challenges for the systematic literature review as the search for information security services and their descriptions required a large deal of manual work and searching with single or partial words instead of utilizing the complete terms. Moreover, the use of the shorter term ‘security service’ made it unclear, whether the two terms were utilised as synonyms or whether the former was considered to be a broader term concerning security. Additional challenges were caused by the functionalities of the reference management software that did not recognize terms that were divided into two rows with a hyphen. Thus, it was difficult to ensure that all the descriptions had been identified from the articles. Similarly to the use of the term ‘security service’, only the term ‘service’ was utilized, which again made it cumbersome to distinguish whether the article discussed a certain information security service or some other service. Omitting the services including merely the term ‘service’ instead of a ‘security service’ would have, however, resulted in less findings and a narrower view on the topic. In addition, in some cases the lack of the term ‘service’ proved it difficult to discern whether the article was discussing an infosec service or a description of a function. This can be observed in terms such as ‘authentication’ and ‘authorization’; both of them can be identified as security services and as activities.

These findings prove that a wide range of terms, which are not well-established but often used as synonyms, exist in academic literature. In addition to that, drawing a line between the different terms and deciding which ones could be included in the categorization was often very difficult. Therefore, it remains somewhat unclear, which terms can be utilised synonymously to information security services and which carry a clear distinction. The obscurity in the use of terms supports the fact that it remains ambiguous which solutions can be regarded as services and which not. This was also visible in the previous discussion of the role of confidentiality, integrity and availability (CIA) regarding security services – should they themselves be regarded as services, requirements or as objectives or properties protected by the services? In this study they are considered as all of those attributes. Based on the findings, however, it can be stated, that the terminology in use is very fragmented and lacks cohesion.

Another interesting viewpoint in the SLR was the level of detail regarding the services. Some articles utilized generic terms whereas others went into more detail with the services. An example of this would be Liping and Lei (2011) that presented terms, such as information integrity and message confidentiality and Rachedi and Benslimane (2016) that utilized terms, such as relayed nodes authentication and integrity, data integrity and end-to-end data confidentiality. The higher level of detail increases the concreteness of some of the otherwise abstract services – a matter which was discussed in the previous section.

### *3.3.6 The significance of security services in the SLR articles*

In addition to the terminology, attention needs to be directed to the handling of information security services in the articles. Based on the review of the articles, information security services were often a secondary theme in the contributions and the articles observed the topic from a limited angle. This means that many of the articles did not provide a comprehensive view or listing of the services but focused only on those services that were relevant and supported the topic of the article. This, in turn, could affect the systematic literature review by distorting the results. Some of the articles, on the other hand, only mentioned a few services as examples of information security services to give a general understanding to the reader. Jeong et al. (2010) and Xia and Hu (2006), for example, briefly mention few security services in their articles. Furthermore, the descriptions of information security services in the articles were often very scarce and shallow. The cursory handling of the topic also affected the identification of services: Deficient descriptions and unclear terms caused problems in the interpretation of information security services. Without a clear description of the service, it was sometimes difficult to deduct what kind of information security services the authors were referring to.

By observing the articles in terms of mere numbers, Wang et al. (2010) and Karyda et al. (2006) provided the most extensive listings of information security services. Furthermore, the additional publication by Buecker et al. (2007) presented a rather wide listing of services. However, if observing only the articles accepted into the SLR based on the handling of the topic, Karyda et al. (2006) presented the most comprehensive view on information security services as they had included both technical services – such as virus protection and disaster recovery – and non-technical services – such as security policy development and training – in the broad list of services in their article. Nevertheless, none of the articles provided a listing of security services that would have included all of the services found during the systematic literature review. On the other hand, this is natural as the number of identified services was high.

Another notable observation was the frequency of the information security services in the articles. Some services were presented more often than others; among the most popular ones were, for example, confidentiality (e.g., Miguel et al. 2015, Peiris et al. 2008 and Rachedi & Benslimane 2016), authentication (e.g., Chappell et al. 1999 and Claassen et al. 1992) and access control (e.g., Oladapo et al. 2009 and Peiris et al. 2008), whereas some services (e.g., traffic pattern by Datta Ray et al. 2010, security upgrades by Karyda et al. 2006 and media protection by Oladapo et al. 2009) were only present in single articles.

As mentioned earlier, the findings from the systematic literature review were utilized in building an information security service categorization. Despite the fluctuations in the

frequency of information security services in the articles, all security services were handled equally in the categorization, even though some sort of prioritization based on the frequency could have been utilized. The equal approach was adopted as the topics of the articles may have influenced the types of services presented and as only few articles centralized on infosec services. The categorization will be presented later in section 3.4. However, before immersing into the categorization, we will first discuss the quality of the SLR articles in the next section.

### *3.3.7 Quality of articles*

The quality of the systematic literature review (SLR) articles is also a matter to be observed. The material in the review varied extensively ranging from articles that expanded on security services and presented rather extensive lists of them to articles that adopted a shallow approach on the topic and presented only few information security services. Additionally, the quality of the text within the articles varied; some articles were well written, whereas some were cumbersome to read and understand. This may have had an impact on the security services identified. However, as stated earlier, the quality of the articles was evaluated during the SLR process and some articles were omitted during the SLR due to poor quality.

From an academic point of view, the quality of the publications was reviewed through JUFO publication channel ranking. JUFO ranking, published by Publication Forum (Julkaisufoorumi), promotes the quality assessment of scientific research (Home 2017). The ranking evaluates both Finnish and foreign publication channels on a scale from 0 to 3 from which 2 and 3 represent the publication channels that are most influential or follow the highest standards. Level 1, in turn, consists of peer-reviewed publication channels that specialize in publishing scientific research results. Furthermore, level 1 is the basis for publication channels, whereas level 0 is given to publication channels that do not fulfil all of the requirements of level 1. (Evaluations 2017.)

For most of the articles (31 out of 36), the publication channels were not found in the JUFO ranking database. For five of the articles, however, the level of rating for the publication channel was 1. One of the reasons for the lack of ratings was the fact that JUFO ranking only showcased ratings for publications from 2012 onwards. In fact, most of the articles (27 out of 36) were published prior to that year (division of publications per year was depicted earlier in Figure 6). This could affect the lack of ratings in the articles. Furthermore, for seven of the articles without a rating, the publication channel had received a rating of 1 from 2012 or 2013 onwards. For two of those publication channels, the rating had been raised to 2 from 2015 onwards. For one of the SLR articles, the publication channel had received a rating of 2 between years 2012–2014 and a rating of 3 from 2015

onwards. For seven of the SLR articles, the publication channels had received a level 0 rating from 2012 onwards or later, referring to incomplete fulfilment of level 1 requirements. The ratings of the publication channels for the SLR articles have been depicted in Table 11.

Table 11 JUFO ranking

| Level | No rating | Level 0 | Level 1 | Level 2 | Level 3 | In total |
|---|---|---|---|---|---|---|
| **Number of publications** | 31 | - | 5 | - | - | **36** |
| **%** | 86.1% | 0.0% | 13.9% | 0.0% | 0.0% | **100.0%** |

From the academic evaluation perspective, the quality of the articles leaves room for improvement. However, the ratings from 2012 onwards showcase that many of the publication channels have later been recognized as meeting the basic level requirements of the JUFO ranking and, thus, obtaining sufficient quality. Additionally, it must be noted that the lack of found ratings does not automatically signify that the publication channel does not have one; this could be caused by the use of search terms. However, this proves that the article base included in the systematic literature review was rather divided and that the articles have not been published in high-quality publication channels. These results could support the earlier notions of the inconsistent quality of the articles and of the varied handling of the topic in them.

## 3.4 Information security service categorization (ISSeCa)

### *3.4.1 The ISSeCa building process*

Before presenting the ISSeCa categorization in more detail, it is useful to first observe the building process of the model. The categorization was built in the form of a mind map. According to Siekkinen (1997), there are various types of concept or mind maps; the type utilized in this study represents one of them. However, instead of utilizing symbols, colours or linking phrases, which are notation types utilized in concept maps (Siekkinen 1997), the categorization built in this study only includes concepts – the infosec services identified in the systematic literature review (SLR) – and links that represent relationships between the concepts. Furthermore, there are various strategies for building a mind map (e.g., mapping by core idea or author as is presented by Machi and McEvoy

(2009, 49–50)). Siekkinen (1997) discusses deductive and inductive approaches to building mind maps from which the prior first builds the basic structure for the map, whereas the latter begins by identifying concepts through a thinking process and based on those concepts, determines the main categories to which the concepts are then placed. The strategy used in this study included both inductive and deductive elements as the main and subcategories were determined before placing the services into the structure. However, the insights from the SLR inevitably influenced the selection of the types of categories. In fact, the thinking process behind the building of the mind map can be rather multifaceted (Siekkinen 1997). The categorization building process is presented phase by phase next; additionally, the whole process is pictured in Figure 8.

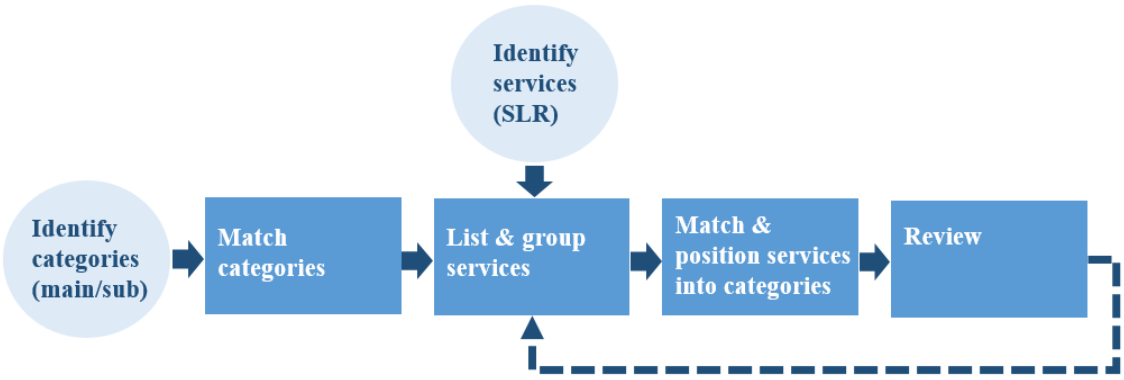



Figure 8 ISSeCa building process

The building of the categorization began by identifying suitable models for categories. Multiple possibilities for the categories were considered: the perspectives identified in the SLR (1), self-made categories (2) and the components of the CIA triad (3). However, all of the three possibilities had to be abandoned. Firstly, although the SLR perspectives offer useful insights into infosec services, they were not chosen as the categories of the ISSeCa categorization as they are too generic. Secondly, utilizing a mere self-made categorization could have caused unbalanced categories and, thus, an unbalanced categorization. Thirdly, utilizing confidentiality, integrity and availability (CIA) as the categories proved to be impossible as many services can be construed as supporting several of these characteristics. However, this can be interpreted as a prominent finding as it showcases that security services are not one-sided but help in enabling information security in a more versatile manner.

After observing the various possibilities for the categories, the 14 security control clauses of the ISO 27002 standard were found and chosen as the categories of ISSeCa. However, it soon became evident that the high number of categories made the structure too scattered: The clarity and usability of the categorization had to be enhanced and, thus,

the eight information security categories presented in VAHTI instructions were determined as the main categories of ISSeCa. Furthermore, the security control clauses of the ISO 27002 were then named as the subcategories of the model.

Even though the chosen models – ISO 27002 standard and the information security areas by VAHTI – are non-academic, both the International Organization for Standardization (ISO) and the Ministry of Finance in Finland are well established. The information security areas seem to be mainly utilized in Finnish literature sources but the standards by ISO are acknowledged and sought after by organizations worldwide. In fact, according to SFS-ISO/IEC 27000 standard, the ISO 27002 standard presents generally accepted control targets and best practices for information security mechanisms to be utilized in the selection and implementation of security mechanisms needed to obtain information security (SFS 2012, 24). Therefore, both frameworks suited the purpose of the categorization well.

After identifying the main and subcategories, they had to be matched to form the basis for the categorization. The matching of the main and subcategories was done based on both analysing the descriptions and similarities of the categories in literary sources and the researcher's own discretion; more detailed information on the matching is presented in the next section (3.4.2) for each main category. In brief it can be stated, that the matching of subcategories and, in fact, the building of the whole categorization follows the notions of Machi and McEvoy (2009, 49–50): The authors state that “each of the categories or parts that make up the core idea should be sketched as subsidiary, or supporting, idea”. Thus, the different levels of the categorization construct the higher levels from sub- and main services through sub- and main categories up to the main topic of the categorization. An example of this chain is presented in Figure 9 by referring to the Personnel security branch from the ISSeCa categorization.

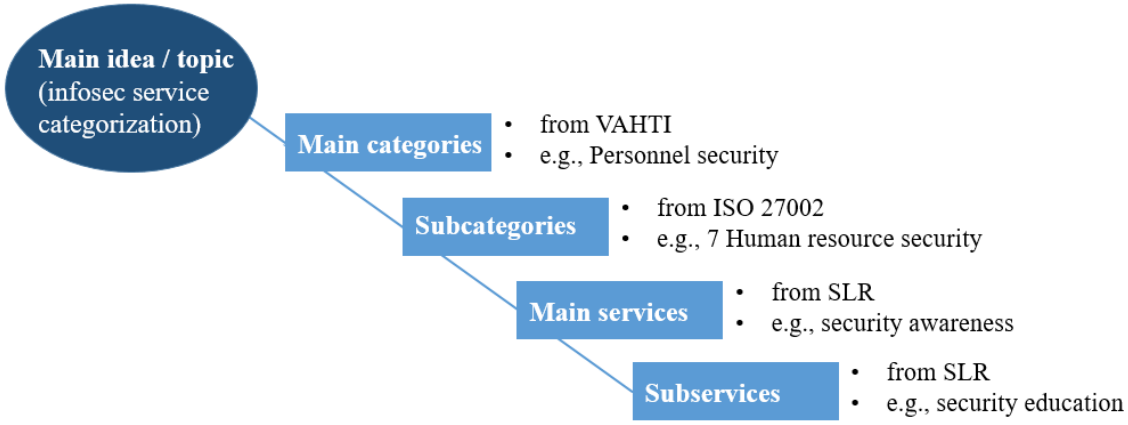



Figure 9 ISSeCa branch structure

After matching the main and subcategories, it was time to focus on the services identified in the SLR. In order to position the services into the categorization, it was important to understand the purpose of the services. However, the context and descriptions of the services in the articles were often narrowly presented. Moreover, the researcher did not possess extensive background information on the identified services. Therefore, internet sources were utilized to more profoundly understand the purpose of individual services and to find similarities or interconnections between the services for grouping purposes. Similarly, descriptions of the frameworks in both the ISO 27002 standard and VAHTI instructions were utilized to guide the grouping of the services. During this phase, the services were listed, grouped and, finally, nominated to subcategories in Excel. Novak and Cañas (2008, 12) also suggest listing the different concepts identified; however, instead of grouping the services they take the idea further by suggesting listing them from generic ones to specific ones to ease the mapping.

After the service grouping phase, the services were individually transferred to the categorization mind map. The more generic or comprehensive services were nominated as the main services of different branches under subcategories, whereas the more detailed services were placed under those main services in the branches. Simultaneously, the balanced nature of the categorization was supported by choosing similar types of services as the main services of each branch under a subcategory (e.g., encryption services, firewall management and audit services as the main services and the more detailed packet encryption, firewall configuration and IT auditing as their subservices). This approach to the building of the categorization is supported by both Novak and Cañas (2008, 1–2) and Siekkinen (1997) from which the latter states that a mind map is construed of a central concept which is further divided into main and subconcepts or paths.

Expert reviews on the categorization were unavailable and, thus, peer reviews from a person with several years of experience in the field of IS was utilized instead in order to help detect inconsistencies in the placement of services. The forming of the categorization

was done iteratively as it was refined based on new found information and increased understanding on the topic. Additionally, new services were identified from the SLR articles and added to the categorization during the process. The iterative nature of the building process is supported by Novak and Cañas (2008, 12), who state that the initial concept map should always be revised, during which new concepts can be added. According to the authors, a finished concept map does not exist. It should also be noted, that the ISSeCa categorization presented in this study is only one way of classifying these services; in reality, the categorization could have been built in multiple ways. This thought is examined in more detail in section 3.4.3 when reflecting on the building process.

### *3.4.2 Description of ISSeCa*

This section presents the information security service categorization (ISSeCa), which is built from the infosec services identified during the systematic literature review. The categorization is based on two different models: the information security areas presented in VAHTI instructions and the security control clauses of the ISO 27002 standard. VAHTI instructions, that consist of eight information security areas (Classification of instructions, 2017), form the main categories, whereas the ISO 27002 standard, which includes 14 clauses (ISO/IEC 27002, 2013), form the subcategories of the categorization. Both of the models have been described in detail in section 2.3. Figure 10 depicts the main categories of the ISSeCa information security service categorization.

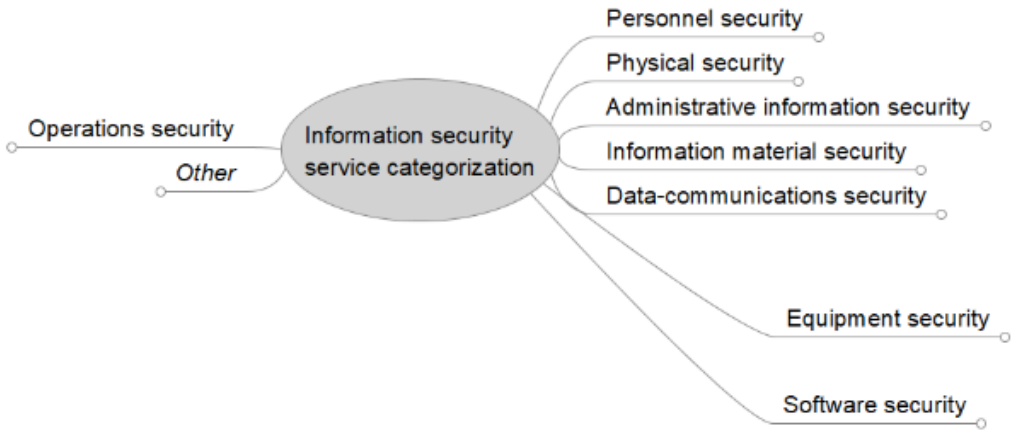



Figure 10 ISSeCa: Main categories (based on Classification of instructions, 2017)

In addition to the eight main categories, a category 'Other' was included in the categorization to enable the inclusion of information security services that did not apply to any of the existing categories. Next the thesis will further examine these main categories and their subsidiaries; furthermore, excerpts of the categorization in picture form will be

presented. The entire categorization containing all of the accepted services is available in Appendices 1.0–1.5; additionally, Figure 21 presents an overview of ISSeCa at the end of this section. It is noteworthy to mention, that terms in *italics* in the categorization are not infosec services identified during the SLR but additional titles to support the structure of the categorization. The subcategories follow the numbering utilized in the ISO standard (ISO/IEC 27002, 2013); an outlook of the subcategories of ISSeCa has been depicted in Figure 11.

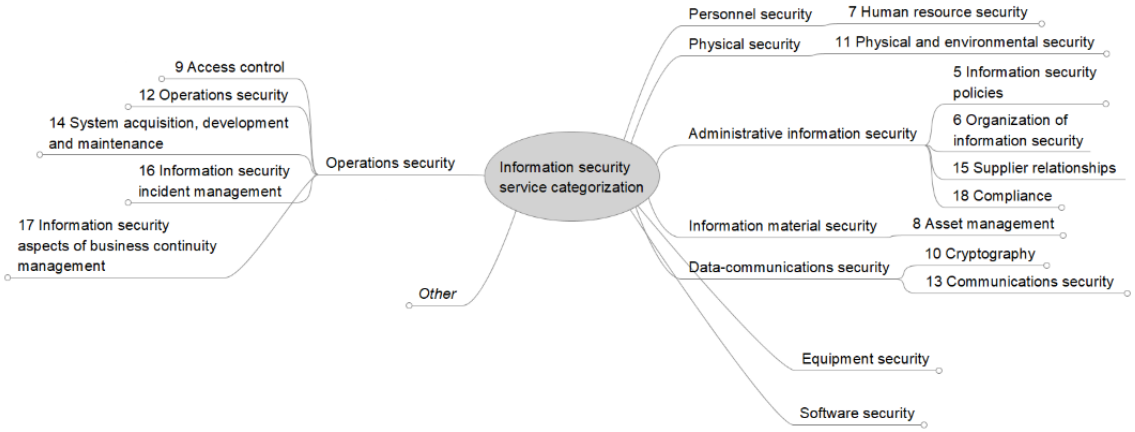



Figure 11 ISSeCa: Subcategories (based on ISO/IEC 27002, 2013)

The first main category, *Personnel security* includes subcategory Human resource security (7), whereas the second main category, *Physical security*, includes the subcategory Physical and environmental security (11). Human resource security was placed under the prior main category as they both address similar, people-related issues; Physical and environmental security, in turn, was placed under the latter main category as they both handle physical security related topics. Both of the subcategories consist of a limited amount of services: The prior category includes softer security services related to people, awareness and security education, whereas the latter focuses on physical security services. These services have been pictured in Figure 12.

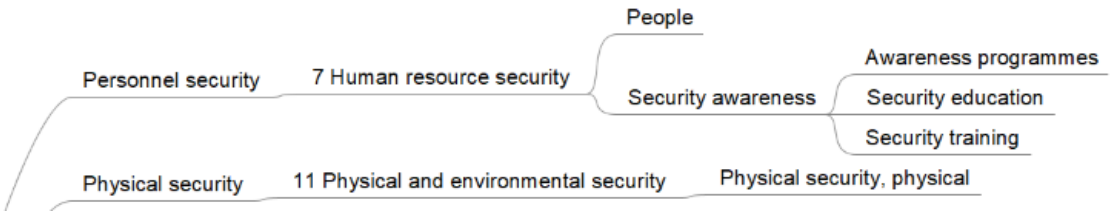



Figure 12 Personnel security & physical security

The third main category, *Administrative information security*, includes subcategories Information security policies (5), Organization of information security (6), Supplier relationships (15) and Compliance (18). *Information security policies* includes services related to policies and policy management, whereas *Compliance* concentrates on guidelines and documentation, governance, certification and privacy. These subcategories were included into this main category as they can be regarded as categories addressing management-level information security issues and overall information security management. It is noteworthy, that the two remaining subcategories – *Organization of information security* and *Supplier relationships* – do not include any information security services as no suitable services were identified. Nevertheless, the categories were retained in the categorization to ensure a balanced model. The services of the third main category are depicted in Figure 13.

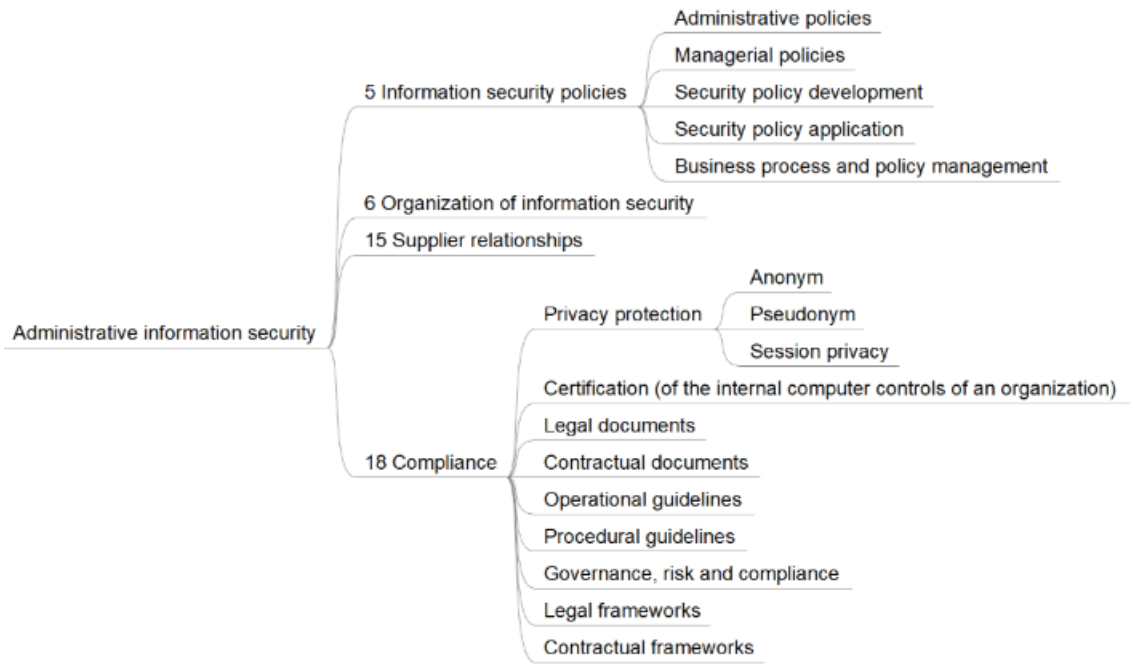



Figure 13 Administrative information security

The fourth main category, *Operations security*, focuses on the operational side of systems and includes the highest number of subcategories. These subcategories include Access control (9), Operations security (12), System acquisition, development and maintenance (14), Information security incident management (16) and Information security aspects of business continuity management (17). The aforementioned subcategories were placed under Operations security as they can be regarded as supporting the operative, daily management of information security in comparison to the more strategic information security management under Administrative information security. These services address daily infosec issues, such as access control, security analysis, incident management and security upgrades encountered within an organization. On the other hand, ensuring business continuity is also included in this main category as it can be regarded as an important part of operative information security.

From the above listed subcategories, the category *Access control* (Figure 14), includes services from the areas of access control, identification, authentication and authorization as they can be interpreted as forming a group or process of access control related security services. The linking and threading of these services was also proposed by multiple authors in the systematic literature review (e.g., authentication and authorization by Kovač & Trček 2009 and Asgarnezhad et al. 2010, identification or identity management and authentication by Miguel et al. 2015 and Jin et al. 2003 and authorization and access control by Shaikh et al. 2005). Furthermore, services regarding user provisioning and passwords are included in the subcategory. The second subcategory, *Operations security*, in turn, consists of topics related to operational information security: audit, server and configuration management, monitoring, vulnerability management, helpdesk and virus

protection services, from which monitoring also includes intrusion detection and behaviour analysis related services. Additionally, security system management related services are placed into this subcategory. A detailed list of services included in these two subcategories is pictured in Appendix 1.1.

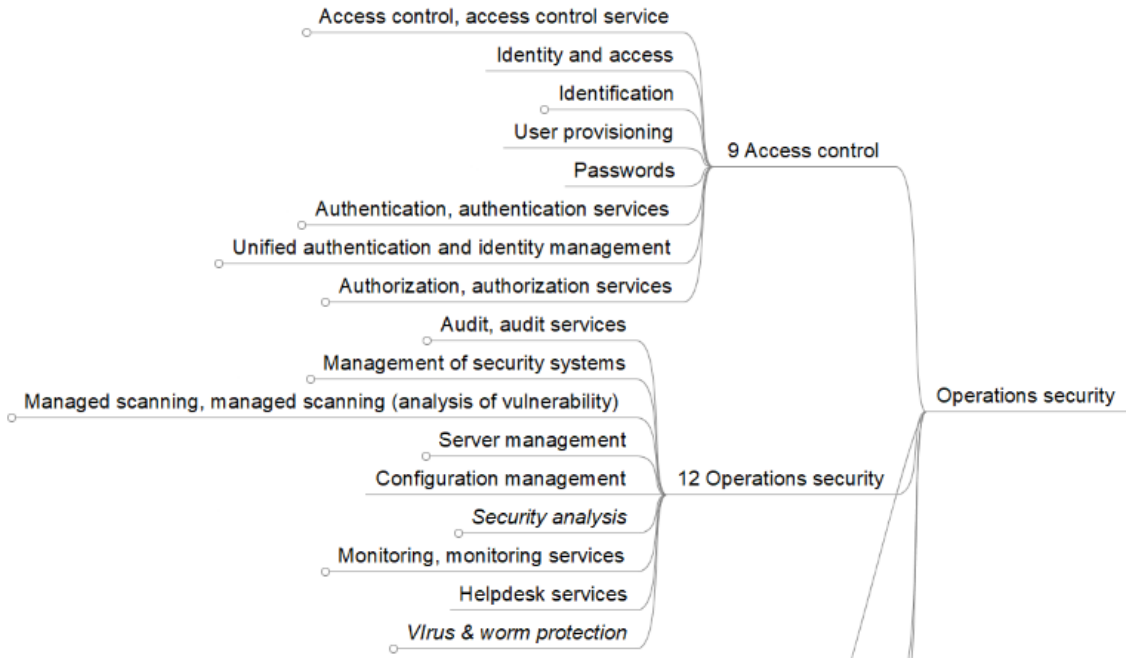



Figure 14 Operations security (part 1)

From the remaining subcategories of Operations security, *System acquisition, development and maintenance* subcategory, on the other hand, includes services related to the management of systems, such as system integration, upgrades and penetration testing. *Information security incident management*, in turn, contains security attack analysis and emergency response services. The final subcategory under Operations security, *Information security aspects of business continuity management*, consists of services aimed at ensuring business continuity. Examples of these services are backups, contingency planning and failure control. All of the services positioned in these subcategories are depicted in Figure 15.

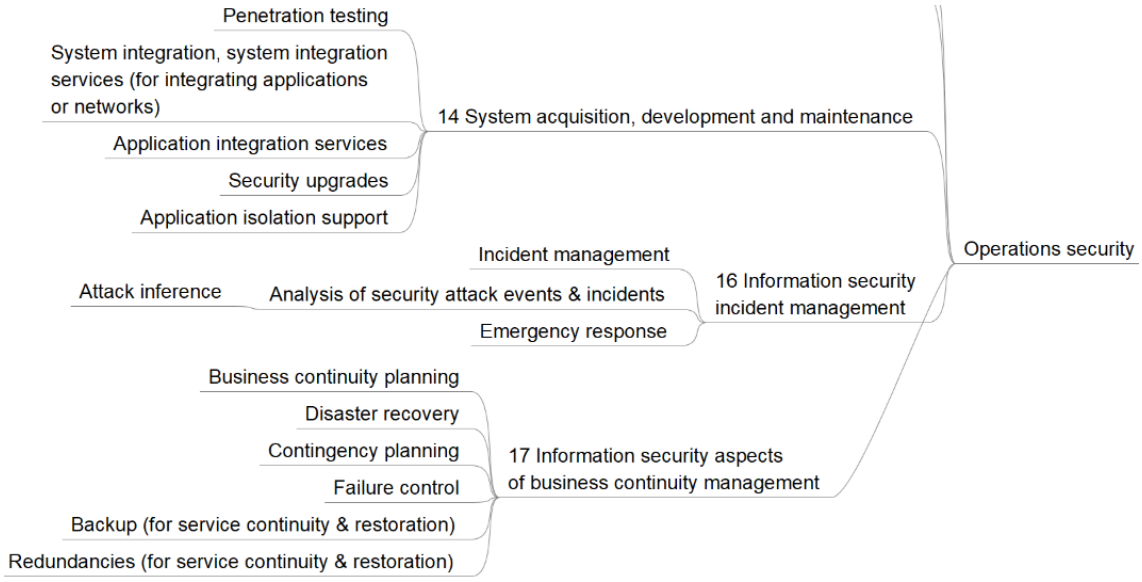



Figure 15 Operations security (part 2)

The fifth main category, *Information material security*, includes subcategory Asset management (8), which consists of services related to data handling, management, storing and protection (Figure 16). These services include, for example, data archiving, restoration and time stamping. Asset management was placed under Information material security as the ISO 27002 describes information as one type of business asset to be protected against threats (ISO/IEC 27002 2013, vi). The placement of the subcategory under this main category is justified as the ISO standard (ISO/IEC 27002 2013, 15–18) includes the classification of information and handling and disposal of information stored on media within asset management.

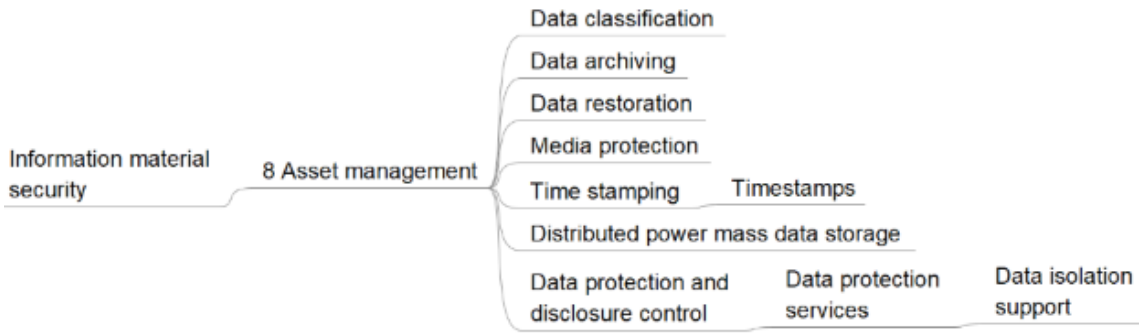



Figure 16 Information material security

The sixth main category, *Data-communications security*, in turn, includes subcategories Cryptography (10) and Communications security (13) (Figure 17). The prior includes services related to encryption, algorithms, public key infrastructure, digital signature and security protocols, whereas the latter consists of services related to networks, filtering,

firewalls and virtual private networks. Furthermore, network services contain several topics, such as cloud security, decoy services and threat detection. A complete list of the services placed under these subcategories is available in Appendix 1.3. Cryptography and Communications security were placed under the Data-communications security main category as they both aim at ensuring the safe transfer of information. VAHTI also relates encryption, which is placed under Cryptography in ISSeCa, to data transfer safety (Valtionhallinnon tietoturvasanasto 2008, 103); this further supports the placement of the Cryptography subcategory.

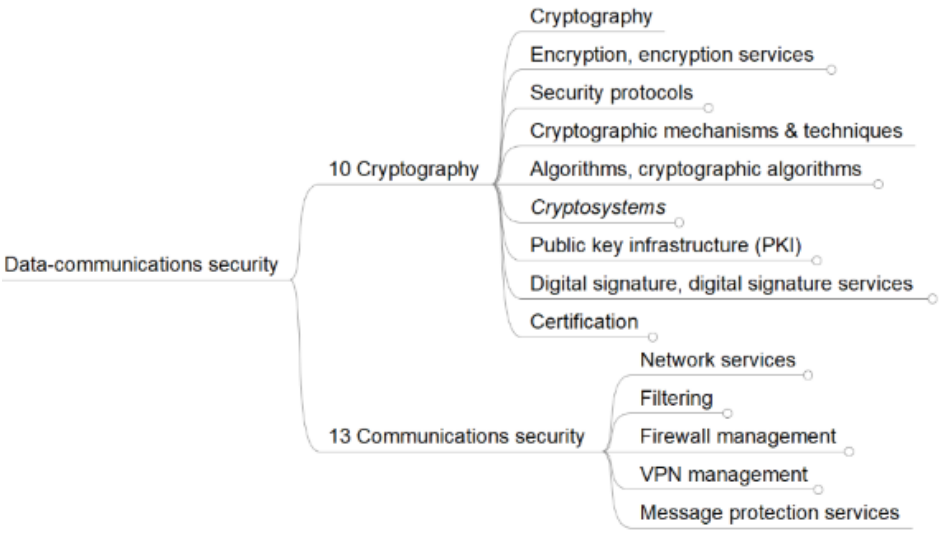



Figure 17 Data-communications security

The seventh and eighth main categories, *Equipment security* and *Software security*, do not contain subcategories (Figure 18). The latter is, to some extent, unnecessary as many of the security services are software. Nevertheless, these categories have been preserved in the categorization as suitable infosec services were identified. Equipment security includes services related to hardware, equipment in general and maintenance as it refers to the maintenance of equipment. The placement of security maintenance is not unambiguous as the service could have been placed under Operations security as well. The services placed under Software security, in turn, include software and applications related services as they can be regarded as being closely linked to the subcategory.

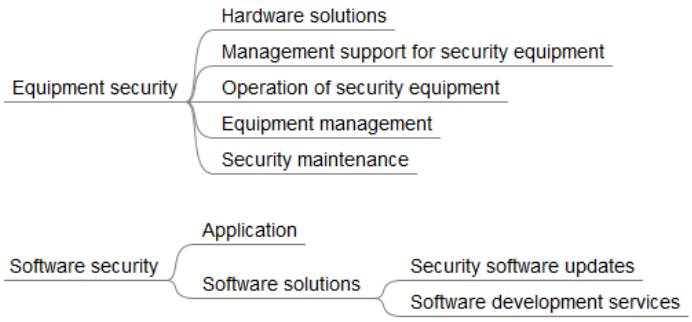



Figure 18 Equipment and software security

The final main category, *Other*, in turn, includes the following subcategories:

- CIA
- Consulting
- Trust & norms
- Classifications & descriptions.

It is notable that the subcategories in this main category are not based on the ISO 27002 standard but are determined from the findings of the SLR; all of the ISO subcategories have been included in the preceding main categories. The subcategory named 'CIA' includes those information security services that simultaneously describe information security: confidentiality, integrity, availability and non-repudiation (Figure 19). The category also includes the more detailed variations of these services. As these services are highly abstract, and thus very different from many of the services identified, they could not be positioned under any of the VAHTI main categories. Additionally, services related to trust, consulting and consolidated billing have been placed under the main category due to their abstract nature or discrepancy form other identified services.

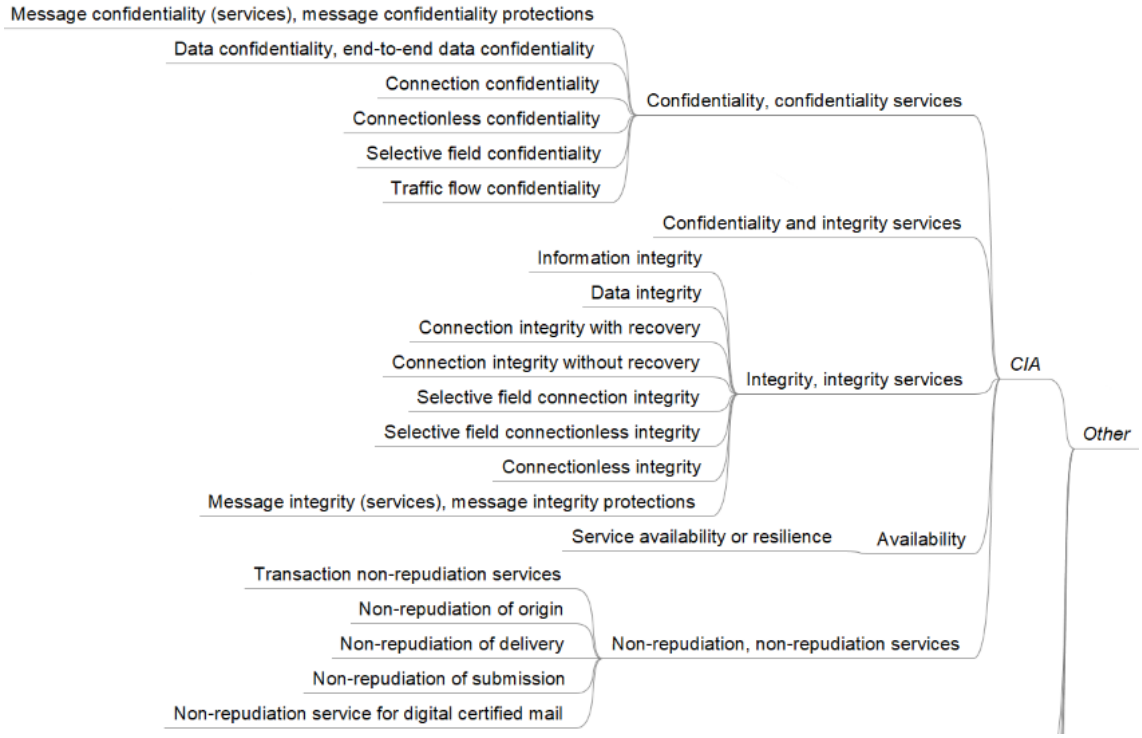



Figure 19 Subcategories and services in main category *Other* (part 1)

Similarly to *CIA*, the subcategory ‘Trust & norms’ includes ethical and cultural norms and trust, which are abstract services. In addition to those services, *Trust & norms* includes trust and reputation systems which refer to the rating of services (Figure 20). Other subcategories and services under the main category *Other* include the above-mentioned consulting related services and consolidated billing. Furthermore, the classifications found in the systematic literature review have been included under the ‘Classifications & descriptions’ subcategory, even though they do not represent individual services. This subcategory also includes descriptions or types of services found from the SLR articles. A complete list of the contents of *Classifications & descriptions* is available in Appendix 1.5.

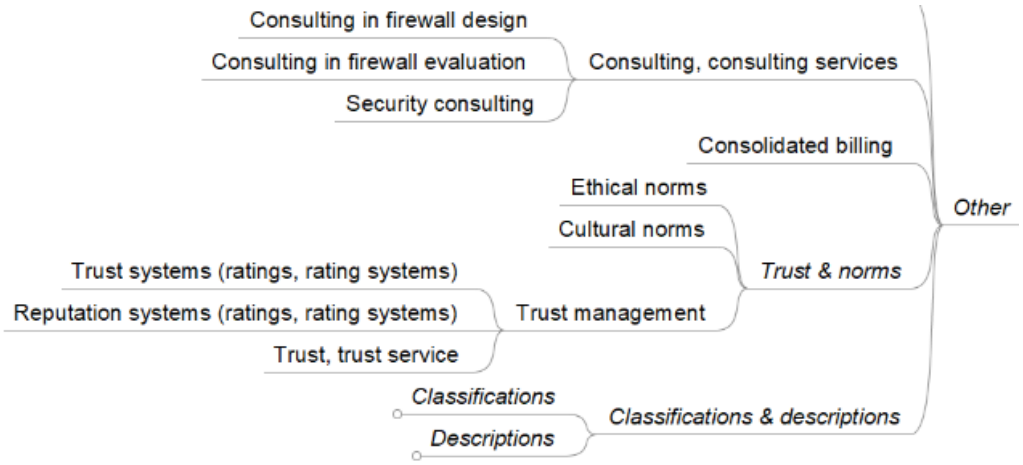



Figure 20 Subcategories and services in main category *Other* (part 2)

As a conclusion of ISSeCa it can be stated, that the categorization aims at incorporating the different types of services identified during the SLR as is visible from the overview of the categorization in Figure 21 below. To a large extent, the two information security models – VAHTI and ISO – have enabled this. However, the services are not equally divided between the categories. In fact, *Operations security* and *Data-communications security* are the largest categories in the categorization based on the amount of services included in them. In terms of subcategories, *Operations security* and *Administrative information security*, in turn, are the largest main categories with five and four subcategories. The extensiveness of *Operations security* and *Data-communications security* categories demonstrates the dominance of the hard, technically oriented services and, therefore, naturally supports the findings of the systematic literature review: The softer security services represent a minority in the categorization by being included mainly in the *Personnel security*, *Administrative security* and *Other* categories; similarly, the amount of physical security services is scarce. On the other hand, the amplitude of *Operations security* is understandable when considering the recommendation of Hakala et al. (2006, 12) of incorporating operations security in all of the other areas of information security. This demonstrates the importance of this security area and, thus, supports its wide scope. Next we will reflect on the complexity of the categorization building process.

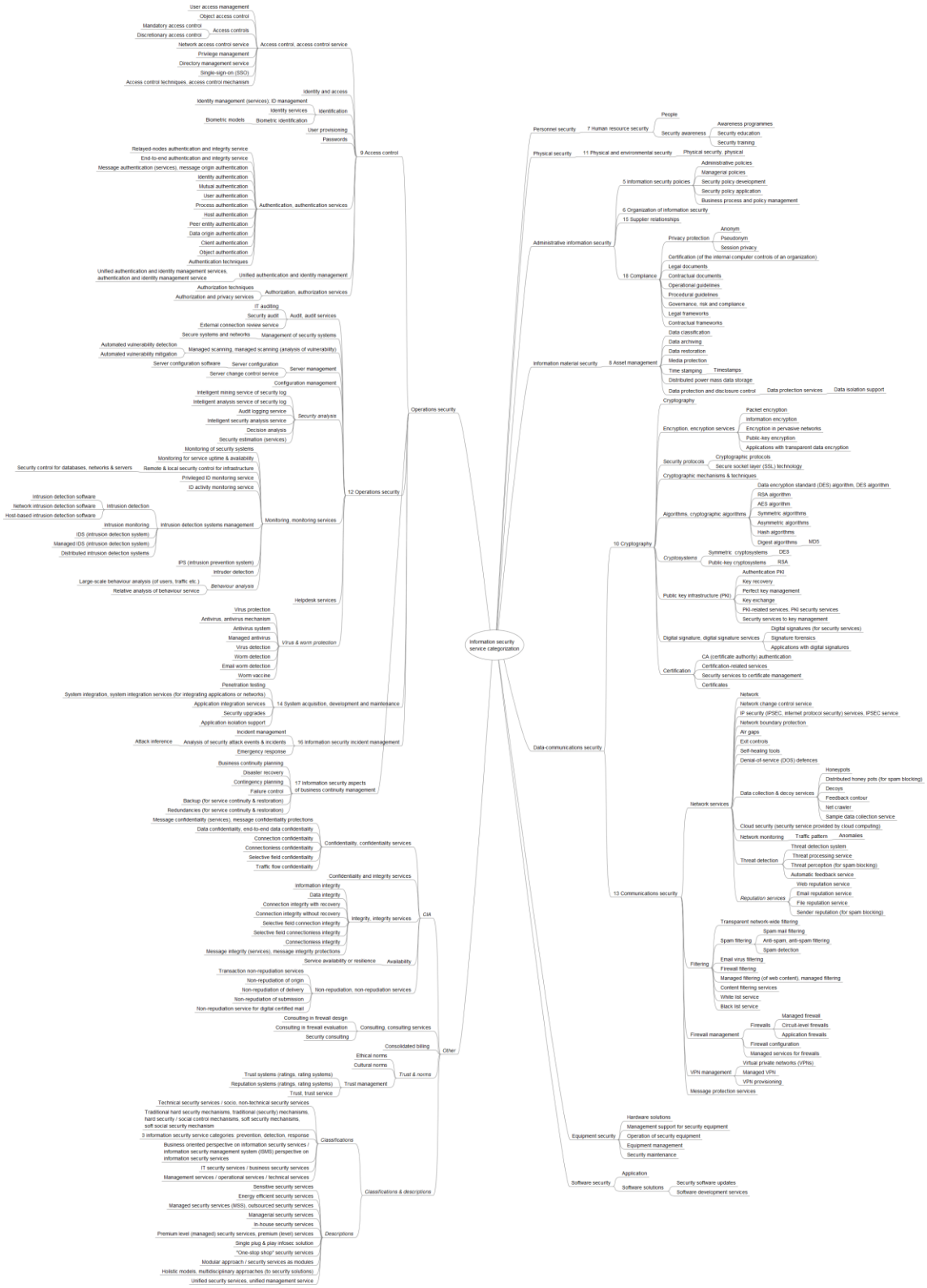



Figure 21 An overview of the ISSeCa categorization

### *3.4.3 Reflections on the forming of the categorization*

The ISSeCa categorization offers one way of presenting the information security services identified in the SLR in a structured manner. However, as noted above, this presentation is not absolute and various compromises in the building of the categorization had to be done. This section provides insights into the perceived diversity of the services during the building process.

First it is useful to note that the positioning of the subcategories and security services was not unambiguous due to linkages between the services. The subcategory *Supplier relationships (15)*, for example, could have been positioned under *Operations security* as it could be interpreted as operative supplier management in addition to the administrative management of suppliers. From the service point of view, there were numerous services with multiple possible locations in the categorization. To name a few, examples of such services include firewall filtering, which is connected to both filtering and firewalls, monitoring which could refer to the monitoring of systems or services and, thus, be linked to both of them, and intrusion detection, traffic patterns and anomalies which could be linked to both networks and monitoring. Protocols, on the other hand, could refer to administrative security or cryptography, whereas digital signatures could be affiliated with cryptography, algorithms or authentication. Finally, privacy could be linked to either cryptography or to the data privacy of individuals, from which the former adopts a technical and the latter a more people-oriented perspective.

A similar situation occurred with different groups of services. The positioning of the CIA services, for example, was difficult due to their abstract and networked nature. The newly established category *Other* proved to be the most natural position for these services. Managed security services, on the other hand, could have been combined under one root in the categorization as they form a distinctive group but, instead, they were divided into different categories based on the purpose of each service.

Another difficulty emerged in the positioning of those services that integrate several different services. An example of this are services that combine authentication and integrity described by Rachedi and Benslimane (2016) or the unified authentication and identity management services introduced by Jin et al. (2003). Despite the multifaceted nature of these services, they were only placed into the categorization once and the position was determined by the discretion of the researcher. Dotted lines between subcategories could have been added to the categorization to demonstrate the linkages between the services. However, when tested, this made the categorization confusing and, thus, the lines were abandoned.

These examples prove a widely spread network of linkages between the services. In the end, all of the services are connected as they aim at fulfilling the same goal – preserv-

ing critical information and protecting it against harm. Therefore, the networking of services is understandable. In fact, Novak and Cañas (2008, 12) support this insight emerging in the building of concept maps by noting that it is important to understand that "all concepts are in some way related to one another". On one hand, due to the networked nature of the services, the categorization could be interpreted as somewhat artificial and incomplete as all of the connected services could not be properly linked in the categorization and as the positioning of the services is debatable. Hakala et al. (2006, 12) support this notion of artificiality by stating that, in reality, all of the information security areas influence each other and share common factors. On the other hand, the division of these areas helps in information security planning (Hakala et al. 2006, 12). In conclusion it can be stated, that the categorization provides excellent insights into understanding the nature and connectedness of information security services. These findings also support the earlier notion according to which singular services cannot guarantee the security of information assets but, instead, a compilation of security services should be gathered and implemented based on the needs of the organization. After presenting the ISSeCa categorization, the study will now concentrate on the survey part of the research.

# 4 SURVEY

Based on the categorization of information security services created in the previous section, a survey including quantitative and qualitative questions was conducted to gather more information regarding information security services. This chapter presents the process, analysis and results of the survey; we will begin with the description of the survey process.

## 4.1 Survey process

The questionnaire for the survey was created in Finnish utilizing Webropol survey and analysis tool. The questions were based on the systematic literature review (SLR) results and the ISSeCa categorization as the idea was to deepen the earlier obtained knowledge regarding information security services. Additionally, prior studies were utilized when designing the questions. The survey included cover (Appendix 3.1) and thank you notes and two main sections: The first part collected background information, whereas the second part focused on content questions. Simpler questions were placed in the beginning of the questionnaire to ease respondents and to create a more confident feeling for them regarding the questions; this is also recommended by Heikkilä (2008, 49) and Hirsjärvi et al. (2003, 190).

The background questions examined the role of the respondent within the company, company size and industry. The classification of company size was based on the division utilized by Tilastokeskus (Pienet ja keskisuuret yritykset 2017, Mikroyritys 2017); it includes four classes based on the number of employees in the company. These four classes represent micro companies (less than 10 employees), small companies (10–49 employees), medium-sized companies (50–249 employees) and large companies (250 employees or more). Originally the definition also depends on the turnover or balance sheet total and the independence of the company but, for reasons of clarity and for the ease of the respondent, only the size of the company was taken into account in the question. A prior information security study conducted for Finnish companies by CGI (CGI – – 2016) was utilized when determining the options for both the role of the respondent within the company and the industry categories. The following options were given for the role question:

- business executive
- business expert
- IT executive
- IT expert
- information security executive
- information security expert

- other.

A condensed list of the industry categories was chosen to support the anonymity of the companies as more detailed information might have enabled the identification of the company. The list of industries utilized in this study includes eight categories as follows:

- manufacturing and transport
- trade and services
- healthcare and welfare
- banking and insurance
- IT and communications
- public administration and defence
- energy and water
- other.

To ensure the anonymity of the respondents and their companies, the survey was conducted anonymously and no other background information of the companies was collected.

The content questions consisted of four groups: First group included questions that handled information security services and their importance, the second group handled managed security services, the third investigated competence and investments related to security services and the final group included a question with which the respondent could give feedback and ideas. The content questions included both multiple choice and open-ended, descriptive questions; as the number of questions varied based on the answers of the respondent, the questionnaire did not include numbering of the questions. The questions and the complete questionnaire can be observed in Appendix 3.2. The list of individual security services is wide; therefore, to enhance the clarity and usability of the questionnaire, the main categories of the information security service categorization (ISSeCa) were utilized instead; these categories are presented in section 3.4.

The aim of the survey was not only to find out what kind of information security services the companies utilize but also to measure the importance of the services to those companies. Additionally, as the components of the CIA triad of information security – confidentiality, integrity and availability – clearly emerged as security services, a question to investigate services that support these characteristics was also included. The most important questions were marked as compulsory to ensure answers to those questions. Furthermore, the questionnaire was tested before release.

The population for the survey consisted of companies operating in Finland, whereas the sample comprised 15 responses. The questionnaire was distributed through email and LinkedIn and Facebook social media sites between 15.5.–31.5.2017. During this timeframe, reminders regarding the post in social media were sent, likes for the post were gathered to increase visibility and invitations to answer the survey was distributed via a small group of researchers and other actors. This was done to increase the number of

responses to the survey. The initial goal was to collect a wide sample of companies across Finland by utilizing the network of a partner company, but this proved to be infeasible as the company was unable to participate in the survey process. Therefore, the research focused on companies that could be reached through contact networks and social media sites.

Despite the effort to distribute the survey, it reached a rather low number of 15 responses. The survey was opened but left unanswered over 130 times; therefore, the response rate for the survey was 11.4%, although it is possible that one person has opened the questionnaire multiple times. Additionally, the statistics of the post in social media included 1331 views, 18 likes and 5 reposts in LinkedIn and 45 views in the Facebook page of ICT-portti. ICT-portti is a collaboration programme between companies and universities within Turku area (ICT-Portti 2017); thus, it has the potential to reach a considerable amount of organizations. Due to the low number of responses, the data of the survey was analysed in a qualitative manner instead of the originally planned quantitative approach and colour coding was utilized to support the process. The analysis of the survey will be presented next.

## 4.2 Survey analysis

### *4.2.1 Background questions*

As mentioned above, the first set of questions consisted of background questions. These questions will be handled together next.

The majority of the companies that the respondents presented, operate in the IT and communications industry (9 out of 15 responses). Additionally, companies operating in manufacturing and transport, trade and services, healthcare and welfare and other industries were also present. Furthermore, companies of all sizes were present in the data ranging from micro companies (less than 10 employees) to large companies (over 249 employees). The largest number of respondents were employed in large companies (5 out of 15 responses), although the distribution of respondents between different company classes was quite even. When asking about the role of the respondents within the organization, business executives were the largest individual group with approximately half of the respondents (8 out of 15 responses); however, IT executives, business and IT experts and a development manager were also present in the survey.

### *4.2.2 Information security services and their importance*

The background questions were followed with the first group of content questions that investigated infosec services and their importance to the organization. In the first content question, the respondents were asked to describe in their own words, what they understand by information security services. The responses were rather scattered as they ranged from technical, individual services, such as the virus protection of a computer, through more abstract descriptions of services, such as services that are utilized in protecting information material to holistic descriptions that include many perspectives, such as people, and equipment. We will next explore these answers in more detail.

The most pronounced perspective in the responses was the holistic perspective. This perspective combined people with equipment, properties, software and modes of operation as is visible in one of the responses:

> *[An information security service is] a bulbous entity comprising of matters and services, where the person is in the core and the whole world on the outer circle.*
> (A translated response from a business executive)

Related to the holistic perspective is the finding, that information security services were described as being integrated in the services utilized, ranging from technical platforms to processes. Additionally, infosec services were described as technical, administrative and educational solutions that enable the achievement of business goals.

Describing infosec services with positive terminology related to support was also visible in many responses: Information security services were referred to as services that either protect and safeguard information assets or ensure and improve the information security and ICT entity of the company. Furthermore, infosec services were also characterized as protecting not only the information assets but also the usability and functionality of systems. Additionally, the idea of enabling the use of ICT and the protection of information assets was extended to both the organization and its personnel and to the customers of the organization as is visible in one of the responses:

> *Information security services are services that ensure the use of the ICT entity to both the customer and the staff by protecting and safeguarding the capital of the company and the customer, system usability and operability.*
> (A translated response from a business expert)

On the other hand, infosec services were also described with more negative terminology which is usually associated with control: Information security services were described as being utilized in prohibiting and limiting either the transfer of the internal information assets of an organization to outsiders or the access of malware and outsiders to the systems of the organization. Similarly, these services were defined as technical or expert services utilized in minimizing or managing the information security risks and threats, thus emphasizing a management perspective.

Interestingly, the presence of the confidentiality-integrity-availability (CIA) triad was scarce: One respondent related infosec services to restricting the availability of information, whereas another respondent stated that information security services aim at protecting the secrecy, validity and availability of information assets – properties almost identical to CIA:

> *Services related to IT – especially to information networks, systems and equipment – that are used to protect information capital, its availability, validity and secrecy.*
> (A translated response from an IT expert)

Furthermore, information security services as an outsourced function was mentioned in one of the responses. All participants gave an answer to the question; however, one of the respondents chose to answer 'I don't know'. The aforementioned examples demonstrate that multiple perspectives in defining security services was presented.

Next the respondents were asked to estimate how important information security services are in ensuring the information security of their organization. Most of the respondents felt that the services are very important (10 out of 15 responses), whereas some regarded them as rather important (4 responses). Only one respondent regarded infosec services as neither important nor unimportant for ensuring the information security of their organization. Infosec services are, thus, seen as important in ensuring information security within an organization.

In the third content question, the respondents were presented with the eight main service categories utilized in the information security service categorization (ISSeCa; presented in section 3.4) based on the infosec areas of VAHTI instructions (Classification of instructions 2017). The respondents were asked to determine whether these infosec service categories were utilized in their organization and to evaluate their importance for ensuring the information security of their organization. According to the responses, all of the categories were used in most of the companies. However, equipment, software and data-communications security received the most responses advocating their use, thus, highlighting them as the most common infosec service categories (each received 13 out of 15 responses). This supports the prevalence of technical measures. Physical, personnel,

operations and administrative information security, in turn, were among the categories that received the most ‘not in use’ responses (3–4 responses each). Yet, it must be noted that the differences between the categories regarding the number of responses were scant. According to one respondent, none of the service categories were in use in their organization. Two respondents, in turn, could not specify whether the infosec service categories were utilized in their organization: the first one regarding two categories (information material and administrative information security categories) and the second one all of them. All respondents answered the question.

When evaluating the importance of the infosec service categories, almost all of them were regarded as very important in ensuring the information security of the organization. Two of the categories – physical and operations security – however, were regarded as either rather or very important. In both of these categories, the responses were divided somewhat equally between the two options. It is notable, that in a few responses some of the categories were evaluated as neutral or somewhat unimportant. All of the categories with least importance (‘not at all important’) were given by the same respondent; these three categories included personnel, operations and administrative information security. Furthermore, two respondents evaluated administrative information security as ‘rather unimportant’, whereas physical and operations security were both evaluated as ‘rather unimportant’ by one respondent. Additionally, one respondent could not specify the importance of the administrative information security category. Interestingly, the respondent, according to whom none of the categories were utilized in their organization, regarded all of the service categories as very important to ensuring the information security of their organization. Similarly, the respondent who could not specify whether the service categories were in use, regarded almost all (7 out of 8) categories as very important and the final category, operations security, as rather important. All the respondents answered the question. Based on the results it can be concluded, that all of the categories were regarded as important.

In the next question, the respondents were asked to describe what kind of information security services are utilized to ensure the confidentiality, integrity and availability of information within their organization. For *confidentiality*, services related to access management, such as identity and identity management services, authentication and multifactor authentication, logs and access control were mentioned. Additionally, encryption-related services, such as encryption of mass memories and data communications and secure shell (SSH) and secure sockets layer (SSL) cryptographic protocols, were mentioned. On the other hand, the question was observed through data management: Services, such as data classification and subsequent protection methods and the deletion of obsolete information material, were named as infosec services utilized in maintaining the confidentiality of information.

For preserving the second characteristics, *integrity*, services such as backup on a daily or weekly basis and change log based on classification were mentioned. Additional services for ensuring information integrity included electronic signature, validation sums and software based data storage solutions. Interestingly, one respondent adopted a different perspective on the matter instead of focusing on individual services by suggesting that information security issues should be taken into consideration in organizational processes early on:

> *Relying on the forming of teams and selection of people already from the recruitment phase onwards, often not [relying] on the individual rights.*
> (A translated response from a business executive)

For the *availability* of information, infosec services, such as single sign on, equipment backups, software based data storage solutions and cloud services were named. Other security services included network management services, closed or redundant networks and redundant servers in critical systems and applications, information security software in company network and limiting the amount of open network solutions. On the other hand, contractual aspects and auditing of suppliers, service providers and internal operations were also named as security services enabling availability. One of the respondents described their data as being globally available due to the nature of their business. Another respondent described both integrity and availability as being managed with company resources. Thus, it could be interpreted that they do not utilize infosec services to ensure these information security properties. Only eight participants answered this question from which one informed that they are unauthorized to give a detailed answer to the question due to KATAKRI Finnish national security auditing criteria restrictions. Furthermore, for integrity, only six answers were given. In conclusion, the companies rely mostly on technical services in the preservation of CIA, although examples of non-technical services were also given.

### *4.2.3 Outsourcing related questions*

The second set of content questions focused on outsourcing. In the first question, the respondents were asked to evaluate the level of outsourcing of those information security service categories they had previously named as being utilized in their company. In all of the categories but administrative information security, the services were mainly fully or partially outsourced, from which physical, equipment, data-communications and software security were categories with most responses supporting outsourcing. In the administrative information security category, in turn, the responses between outsourcing and not

outsourcing were equally divided. The majority of respondents answered the question. However, for administrative information security and operations security categories (2 respondents each), as well as for personnel security and information material security categories (1 respondent each), the level of outsourcing could not be determined by some respondents.

Next the respondents were asked to give reasons for the outsourcing of security services; the respondents were allowed to choose multiple reasons from a predefined list or name a reason of their own. The main reasons for outsourcing were the need for flexible and scalable information security resources and services and the desire to focus on the core competence of the organization. Additionally, cost efficiency and the need for cost reductions related to information security and need for wider information security knowledge and know-how were among the main reasons for outsourcing infosec services. Other reasons for outsourcing included the lack of information security know-how or information security resources within the organization, desire for better information security service management and demands from external parties such as customers or laws. Almost all respondents answered the question (14 out of 15 respondents).

### *4.2.4 Information security service competence and investments*

The third group of content questions consisted of questions related to information security service competence and investments. In the first question, the respondents were asked to evaluate the level of information security competence within their organization. Most respondents estimated that the competence within their organization is on a rather or very good level, from which the option 'rather good' was especially pronounced. Some respondents, however, felt that the level of infosec competence within their organization was either on a neutral or rather poor level (5 out of 15 responses in total). One respondent chose the option 'I don't' know'. There was, thus, some deviation in the responses.

Next the respondents were asked to describe the needs of their organization regarding information security services and related competence. Regarding the security services, the respondents named services, such as data encryption, preparedness for denial of service (DOS) attacks, a dashboard service to follow and analyse the information security entity of the organization and more comprehensive information security audits to service providers. On the other hand, one respondent noted that the EU legislation places strict demands regarding, for example, customer privacy – a comment most likely referring to the soon to be implemented general data protection regulation (GDPR) regarding privacy. It could be interpreted that there is a need for infosec services that support the fulfilment of privacy requirements. From a wider perspective, one respondent highlighted the need for development:

> *The development of the processes related to ensuring the information security of the organization.*
> (A translated response from a business executive)

Related to the development perspective is the notion of growth: One respondent noted that the growth of the company could increase the importance of some processes. The responses were, in general, quite fragmented as similar needs did not occur.

Regarding the competence related to infosec services, in turn, the people perspective was pronounced as is portrayed in the following two responses:

> *The general competence and awareness of staff regarding different infosec risks should be improved.*
> (A translated caption from a response of a development manager)

> *The enhancement of the information security knowledge of end users [is] most important and insufficient.*
> (A translated caption from a response of an IT expert)

The respondents described the need to improve the infosec competence of both staff and end users. Additionally, one respondent noted, that the infosec competence is on a good level but as departments do not follow information security instructions, the services do not function as expected. This implies that the infosec compliance should be improved. Another respondent gave an example of the lack of competence by noting that third party follow-up services utilizing cookies may endanger information security but this is not understood [within the organization]. It was also noted that, due to lack of know-how, it is difficult to estimate the fit and adequacy of services which results in relying too heavily on the suggestions of a service provider. On the other hand, the need for more time to concentrate on information security related issues was also recognized as a development area by an IT executive which could imply that more resources towards information security are needed. However, it was also noted that third parties can help with this problem. Finally, the influence of GDPR was also recognized as it acutely poses new demands on information security. The service part of the question received 7 responses, whereas the service related competence part received 6 responses. One respondent could not answer the question due to KATAKRI restrictions.

Next the respondents were asked to describe how they are going to respond to the needs regarding information security services and related competence. Regarding security services, the responses were again quite fragmented. For the preparedness for DOS attacks, partial outsourcing was mentioned, whereas for the need for more comprehensive auditing, finding a new audit partner was proposed. To the services related to privacy

requirements, in turn, it was suggested that more decision power should be granted to the information security department. Regarding the influence of growth in the importance of processes, it was mentioned that the need will be met with internal or managed resources when it occurs, but not in advance. Additional means included built-in information security in internet of things (IoT) devices.

The respondents also named means in responding to the competence needs regarding security services. Additional training to both users and people responsible within IT was suggested regarding the need for both more time for infosec matters and for developing end user competence. Regarding GDPR, in turn, both internal and external auditing and consulting were suggested as means to respond to those needs. Furthermore, one respondent suggested increasing influence as a means to answer to both the infosec service and related competence needs. The service part of the question received 6 responses, whereas the service related competence part received 4 responses. Interestingly, in both of the two previous questions regarding security services and competence, the non-technical, softer needs and measures – such as auditing, training and compliance – were emphasized; this is contrary to the notions regarding the earlier questions of the survey.

The respondents were also asked to evaluate how much their organization is planning to invest in information security services within the next 12 month compared to earlier investments. Most respondents stated that the level of investments will be the same as earlier, although some respondents answered that the level of investments will be somewhat or considerably higher (4 responses out of 15 in total). All of the participants answered the question; 2 respondents chose the option ‘I don’t’ know’. The next section will observe the feedback of the survey.

### *4.2.5 Feedback on the survey*

In the final question group of the survey, the respondents were allowed to give feedback and share ideas regarding the survey. The question received 2 responses. The first response asked for an additional ‘partially in use’ option in addition to the ‘in use’ and ‘not in use’ options – most likely referring to the question of information security service category use within the organization. The respondent continued that most categories are partially in use with known deficiencies. This was further supported by the respondent’s notion that even outsourced information security services are not fully implemented but the level of implementation is decided based on costs. This is a valid feedback and could be taken into consideration in future surveys that further investigate the topic. The more detailed options could provide more in-depth knowledge on the use of information security services; however, it could also make the data more fragmented and results difficult to interpret. For this survey, the current options seemed adequate.

The second feedback noted that due to restrictions set by customers, giving answers to some of the questions was impossible. This notion also emerged in the responses and is a valid finding when considering the low rate of participants in the survey. The low response rate of the survey and reasons for it will be further discussed later in section 5.2. We will further describe the findings of the survey next.

## 4.3 Survey findings

### *4.3.1 An overview of the survey*

Although the amount of respondents in the survey remained low, some findings can be deduced from the data. The main findings of the survey are first capsulized in the below table (Table 12) and then discussed in more detail.

Table 12 Main findings of the survey

| Topic | Main findings |
|---|---|
| Basic information on respondents | • respondents: diverse; half of the respondents were business executives<br>• company size: diverse; companies of all sizes included<br>• field of business: mainly IT and communications field |
| Infosec service description | • many perspectives presented: Mainly holistic, although other aspects, (e.g., technical, developmental) were present; contradictory terminology of support and control (positive / negative)<br>• services named to protect CIA mainly technical |
| Information security categories | • all categories regarded as important; softer categories among those that received most 'not important' and 'not in use' responses, while categories that received most 'in use' responses were all technical |
| Outsourcing | • most categories at least partially outsourced<br>• multiple reasons for outsourcing; mainly need for scalable resources and desire to focus on core competence |
| Infosec importance, level & investments | • infosec services regarded as important<br>• information security mostly on a good level; the majority is not planning to increase investments in information security |
| Infosec service & competence needs | • fragmented needs; non-technical needs and measures emphasized (especially human-related; e.g., training, outsourcing and auditing); GDPR related needs also identified |

First, it is useful to notice that most of the respondents represented business management instead of information security management. This is logical especially in small companies where key roles bear larger areas of responsibility; nevertheless, the data indicated that the division of companies based on size in the sample was quite equal. Closer examination, however, revealed that most of the respondents with business management status represented micro or small companies. The only information security expert in the survey, in turn, represented a large company. These findings indicate that the survey could not reach the persons responsible for information security issues in larger companies to the extent needed or such persons were unwilling to participate in the survey. It is also noteworthy, that instead of achieving a balanced representation of different fields of business, most of the companies in the survey operate in the IT and communications sector. This could lead to more informed answers and higher emphasis on infosec issues than would from companies operating in other fields. This is due to the fact that IT companies are likely to have a better understanding of information security as it often represents one of their core businesses.

The organizations estimated that their information security is on a rather good level and were not planning to increase their investments in the matter. At the same time, information security services were regarded as rather or very important for ensuring information security within the organization. Consequently, the companies did identify both soft and technical development areas regarding information security and related competence, although the softer side was more pronounced in the responses. Furthermore, all of the infosec service categories from the information security service categorization (ISSeCa) were in use in most of the companies and regarded as important.

The services of the infosec service categories were mostly at least partially outsourced due to willingness to concentrate on the core competence of the company, need for flexible and wider resources and infosec competence and cost reductions. Therefore, outsourcing was also regarded as a means for increasing infosec competence. One of the respondents, on the other hand, highlighted an important factor regarding investments in information security: The level of information security might not be executed to the maximum level possible but, rather, is optimized based on costs.

Interestingly, while the survey was being executed, the WannaCry ransomware attack spread to companies worldwide. It was expected that the responses might indicate an increased willingness to invest in information security but this assumption did not emerge from the responses. The initial expectation with the question regarding the importance of infosec service categories was that it would yield more in-depth results by demonstrating clearer differences between the categories. The question might have produced better insights if the respondents would have been asked to set the categories in order of priority as it might have indicated greater division between them. On the other hand, the results

indicate that infosec services as a whole are regarded as important for safeguarding information security. This also supports the notion that a more comprehensive approach to maintaining information security is needed. The key findings of the survey will be discussed in more detail next in three categories: definitions, use and needs. *Definitions* section focuses on discussing how information security services were defined in the survey, whereas *Use* section focuses on the security services reported as being used in the organizations. *Needs* section, in turn, focuses on aspects related to future information security needs and measures to correspond to those needs.

### *4.3.2 Definitions of infosec services*

When examining the depictions of information security services, the first finding is that information security services were described through both positive terminology related to support and more negative terminology related to control. They were characterized as *ensuring*, *safeguarding* and *improving* information security but, at the same time, as *limiting* and *prohibiting* access to information assets from unauthorized parties or malware. Another approach to infosec services was to describe them as means of *managing* business risks and cyber threats. This demonstrates that the terminology portrays infosec services through various lenses.

In addition to the support and control aspects, a holistic perspective highlighting the comprehensive nature of information security services was present in the responses; this description was prevalent in the responses. The holistic approach suggested combining the technical side, such as technical solutions and equipment with people, training and modes of operations. Furthermore, the holistic perspective supported the notion of services as entities that are composed of these differing components. Likewise, other authors, such as Soomro, Shah and Ahmed (2016, 223) in their article concerning a literature review on information security management, endorse the view of a holistic approach.

Related to the holistic approach is the integration of information security issues into the organizational processes early on. In fact, information security issues should be taken into account already in the assessment and development phases of information systems or outsourced services (Effective information security 2009, 27). This is a valuable notion as building information security within information systems and processes may prove difficult later on. Furthermore, addressing information security issues once an information system has already been developed may prove to be very expensive and sometimes impossible (Effective information security 2009, 27). Thus, when the infosec issues are taken into consideration already in the early stages, it will be easier to fit them with the requirements of the system or process.

In addition to the aforementioned approaches, a development perspective also emerged from the responses as some respondents described infosec services as services that improve information security and highlighted the development of information security related processes. Furthermore, it was mentioned that growth could change the importance of organizational processes and, thus, influence the security service needs of the organization. Consequently, information security is not a static condition but a continuously evolving process (ENISA 2006, 8). This is a rather interesting finding, as the developmental approach did not emerge as evidently in the systematic literature review. The existence of the soft, holistic and development approaches indicates that business may have a rather developed understanding of information security services – at least within these organizations.

However, it is noteworthy that the CIA perspective – referring to identifying confidentiality, integrity and availability as infosec services – was substantially weaker in the survey than how it emerged in the systematic literature review. Similar properties were linked to security services in only two responses; however, none of the responses actually identified CIA components as information security services. In this sense, business appears to have a somewhat differing image of information security services compared to academia. This difference is also visible in the definitions of information security services provided by the SLR and the survey: Based on the perspectives presented above, it could be argued that the survey provided a wider definition of information security services than the narrow, technical and CIA infused definitions found during the systematic literature review (SLR) presented in 3.3.2.

### *4.3.3 Use of infosec services*

When moving on from the definitions of information security services and observing the security services identified in the survey, the amount of such services was quite limited compared to the findings of the SLR. Furthermore, although the division of soft and hard security services was visible in the answers, the technical side was more pronounced in the responses. This indicated that organizations are mainly utilizing technical services in preserving CIA. This is a controversial finding when compared to the fact, that many respondents had described information security services more as holistic. An exception to this rule was demonstrated by one respondent who suggested that integrity should be taken into account already in the personnel recruitment phase, thus emphasizing the fact that information security should not concentrate on technical solutions but a wider approach should be adopted.

When further examining the categories that are used by the organizations, similar findings occurred. Although all categories were in use and regarded as important, the categories that achieved most 'in use' responses were all technical, whereas the categories that can be interpreted as more non-technical (personnel and administrative information security), were both among the ones that received most responses of not being in use and not regarded as important. Although the number of responses is scant and evidence subtle, this observation is in line with the findings of the systematic literature review (SLR) and the named security services regarding the prevalence of technical information security services. The two remaining categories that received responses of not being in use, physical and operations security, were also evaluated as slightly less important than the other categories. This again supports the prevalence of technical information security.

Furthermore, the narrow approach in naming security services is an interesting finding, as information security is generally regarded as covering all of the three aspects of CIA and, thus, making it a comprehensive approach. It is also a notable finding when compared to the general perceived importance of all of the infosec categories according to the respondents. However, the mode of the research has most likely had an impact on the results as respondents were not asked to name infosec services in general but to give examples of services relevant to their organization instead. Additionally, the lack of information security expert participants could also explain the narrow results. It is noteworthy, that interviews might have provided more in-depth findings on the security services questions than what the open-ended survey questions were able to offer.

### *4.3.4 Needs regarding infosec services*

The results of the survey reveal a division in the acknowledgement of security services: The *holistic* perspective was pronounced in the definition of infosec services, whereas the services utilized to preserve information CIA were mainly *technical* as was discussed in the two previous sections (sections 4.3.2 and 4.3.3). Yet, the future needs and measures regarding information security services and related competence emphasized the *softer perspective*. This supports the notion that having technical information security services in place is not sufficient but it is of utmost importance to engage people – staff, end users and suppliers – in following the security instructions and requirements of the organization. This notion is supported by other authors as was discussed in section 2.2: ENISA stated that the personnel of an organization expose the organization to higher infosec risks than outsiders (ENISA 2006, 8), whereas von Solms and van Niekerk (2013, 101) discussed the human aspect in cyber security by stating that people can be seen both as a vulnerability and an asset to be safeguarded in cyberspace.

The amount of means to answer the infosec service needs presented, in turn, was quite scarce; additionally, the suggestions were quite generic. This indicates that the respondents may not yet have identified suitable measures in responding to the infosec demands of the organization. However, the suggestions corresponded to the notions regarding the identified needs by highlighting softer measures, such as auditing, training and increased authority. Furthermore, utilizing outsourcing and increased influence of information security were mentioned. Additionally, GDPR related needs where identified in some responses, which demonstrates that at least some organizations in the survey are considering needed measures to respond to those needs. These findings support the notion that the importance of information security and the need to invest in it has been identified.

On the other hand, from the financial investment perspective, the results indicated that only few organizations were planning to invest more in information security services and most companies were planning to maintain previous level of investment. The finding follows the earlier notions of the study conducted by CGI (CGI – – 2016) presented in section 1.1 according to which half of the organizations participating in their study were not planning to invest more in information security, despite the fact that the companies recognized both the increased risk of a cyber attack and the need to prepare for such. Interestingly, a global study conducted by Ernst & Young (Path to cyber resilience – – 2016, 15) in 2016 however noted that, according to 61% of the respondents, budget restrictions were regarded as a major challenge for the infosec operations and their input within the company. Yet, 53% of the respondents reported that their budgets had increased within the last year, whereas 55% reported an increase in the spending within the next year. Therefore, the study by Ernst & Young (Path to cyber resilience – – 2016, 15) indicates that the amount spent on information security globally is on the rise. This demonstrates, that on a global scale companies are more willing or prepared to invest in information security compared to their equivalents in Finland. Static investments in infosec and related services, in turn, may require a new way of allocating resources within information security to enable the additional contributions to soft security or to answer the emerging infosec threats yet to be identified. On the other hand, the current expenditure on information security might already be on a high level in the respondent organizations.

# 5 DISCUSSION

## 5.1 Discussion of the key findings

In this section, the key findings of the systematic literature review (SLR) and the survey will be merged together to answer the research questions presented in section 1.3. The following research questions were placed in the beginning of this study:

- What are information security services and how they can be categorized?
- What are the information security services that are used in companies of different industries in Finland?

The first research question is two-fold: It aimed at both finding what information security services are and how these services can be characterized. This study strived to describe information security services based on the depictions of security services in the SLR and survey and the definitions of a service presented earlier in section 2.4.

Based on the prior discussion on the generic nature of services by Kotler and Keller (2011) and Levitt (1981) presented in section 2.4, information security services can be regarded as perishable, variable, inseparable and intangible: Infosec services occur only when they are being produced or maintained and cannot be stored, the quality of service may vary based on the provider, the infosec services are often produced and consumed at the same time and, finally, they usually cannot be experienced prior to purchase.

Additionally, based on the SLR findings, information security services can be described as services that protect and ensure the confidentiality, integrity and availability of information. These infosec services can include different types of services, such as technical, non-technical and physical security services; furthermore, information security services can be concrete (e.g., training, virus protection) or abstract (e.g., trust, awareness). Furthermore, information security services are often provided by third parties, thus partially or fully outsourced by the organization.

Furthermore, from the survey results it can be added, that information security services are entities that can be integrated in other services and processes and that comprise not only of technical security but also of people and modes of operation; as the services integrate multiple aspects, they can be regarded as holistic. Additionally, they bear many functions of support and control as they protect, ensure and improve information security, information assets and the operability of systems, but at the same time, limit and prohibit unauthorized access to the assets and manage infosec risks.

This conclusion proves that business and academia both have a very fragmented view on information security services and a solid definition of an information security service does not exist – thus, it consists of various characteristics depending on the viewpoint of the observer. However, this is understandable as there is a wide range of different security

services based on their nature and function; additionally, the services may answer to different types of needs, although the ultimate aim – ensuring information security – is the same for all of them. Perhaps due to the versatility of these services, only few clear definitions of these services were found in academic literature: When considering the comprehensiveness of information security as a concept, providing an unambiguous definition proves cumbersome if not impossible.

When observing the nature of information security services, multiple insights were identified. Information security services were characterized through soft and hard approaches, from which the prior emphasized non-technical aspects, such as awareness, trust and education, and the latter the technical aspects and solutions to information security. In overall, the hard, technical perspective was pronounced in the research, although the survey clearly presented the holistic and soft perspectives as well. Outsourcing information security services was also an approach present both in the SLR and in the survey: As was evidenced in the survey, the services are often partially outsourced and the reasons for outsourcing vary. Furthermore, outsourcing enables an organization to focus on its core business and to ensure its information security with the help of external expertise. Another important perspective on infosec services that was present in both the SLR and the survey is the holistic one; this was also utilized in the building of the information security service categorization. A variation of this approach is the integration of different infosec services which was presented in the SLR. The development perspective that highlighted the need for evolution regarding information security and related processes, in turn, emerged from the survey. It can be stated that all of these perspectives complement each other as they present various viewpoints to information security and, at the same time, indicate that information security is a puzzle consisting of multiple pieces that need to be fitted together in an organizational context. Only by building a consistent puzzle can an organization achieve a coherent network of information security. Furthermore, the puzzle cannot be built static but needs to be altered and enhanced based on the current and future needs of the organization.

The most substantial controversy in the results of the SLR and the survey was the reference to confidentiality, integrity and availability (CIA) as information security services. The CIA triad has traditionally been regarded as the description of information security. However, the results of the SLR pronounced confidentiality, integrity and availability as information security services. This evidences a divergence in the interpretations of infosec services between academia and business – the latter does not recognize these attributes as services. The identification of CIA as security services raises concerns: How can information security and corresponding services – or in other words, the aim of infosec and the means to achieve it – be distinguished from each other? It was earlier suggested in section 3.3.3 that the scope of the terms could be utilized in separating the def-

initions from each other: Information security refers to all of the attributes of CIA simultaneously, whereas as services they are independent. As such these services are rather abstract when compared to the more concrete infosec services identified during the research.

Other abstract services also emerged during the research. The existence of the abstract services, such as trust and ethical norms, also raised concerns as they are very different form the concrete ones by nature: Abstract services cannot be bought, however, they can be achieved. These services demonstrate similar problems to CIA: identifying them as something to be obtained would make it cumbersome to separate them from the aim of information security. Perhaps then it would be better to regard the categorization as a collection of aspects to be considered when planning information security instead of focusing on the nature of single services. It can be concluded, that the inclusion of the abstract services into the ISSeCa categorization is debatable. Therefore, these findings of the controversial nature of infosec services remain to be further examined and solved by future research.

The second part of the first research question was concerned with a categorization of information security services; this categorization was built based on the findings of the systematic literature review. The categorization, named ISSeCa, utilizes two types of categories from prior literature: main categories from VAHTI instructions and subcategories from ISO 27002 standard. The ISSeCa categorization presents a holistic approach to information security, consisting of areas such as physical, personnel, operations, equipment, software, information material, data-communications and administrative information security. The ISSeCa categorization is presented in detail in section 3.4 and Appendices 1.0–1.5. Furthermore, the comprehensive nature of the categorization is supported with the findings of the survey that acknowledged the need for a holistic approach to information security services. This notion of the holistic approach confirms the phrase that an entity *is more than the sum of its parts*. It is noteworthy to mention, however, that ISSeCa only presents one method of categorizing infosec services and various other solutions could be presented.

The second research question focused on resolving what kind of information security services are utilized in companies in Finland. The answer to this question was searched through a survey. However, only 15 responses were obtained through the survey and, thus, these results cannot be generalized to the population of companies operating in Finland. Nevertheless, the results indicated that, within the group of respondents, the information security services presented through categories were all utilized and regarded as important within the organizations attending the survey. Therefore, these organizations utilize security services that correspond to the needs in areas of physical, administrative, personnel, information material, software, equipment, data-communications and opera-

tions security – as either outsourced or produced in-house. From these categories, software, data-communications and equipment security were most often in use in the participant organizations. Furthermore, these categories were also among the ones regarded as very important for ensuring information security within the organization. When asking about the future needs regarding infosec services and related competence, however, the softer services and measures were emphasized. This interesting controversy could indicate, that organizations have adopted and value the harder, technical security services but are embracing the fact that softer, non-technical ones are also needed. It could, therefore, be concluded that the organizations are currently utilizing hard security services but recognize the need for softer ones as they perceive information security services in a holistic manner.

Another interesting finding in the survey was that, despite the importance of information security services and the identified development areas, the organizations were not planning to invest more in information security in the future; a result that was also presented in the study conducted by CGI (CGI – – 2016) in section 1.1. This could cause problems in the future as new threats emerge and require the allocation of appropriate resources and investments in information security. On the other hand, it was noted that the level of information security is optimized based on costs.

## 5.2 Limitations and future research

This section discusses the limitations of the study and proposes directions for future research. The topic will be handled by first discussing the study in general, then the systematic literature review (SLR), then the survey and, finally, the infosec service categorization.

The delimiting of the study posed challenges as the topic of the study was too wide in the beginning and had to be narrowed down during the research process. This was due to the fact that the study belonged to a larger research programme given as an assignment from the client. Hirsjärvi et al. (2003, 72) contribute to the discussion by stating that especially qualitative research often requires the researcher to focus or redirect their work during data collection. Specifying the research questions and narrowing down the topic of research are, in fact, among the major challenges of students when writing theses (Heikkilä 2008, 24). Therefore, the changes and delimitations to the study can be regarded as natural during the thesis process. Additionally, the SLR and the forming of the information security service categorization (ISSeCa) proved to be much more laborious than initially expected. Despite theoretical knowledge, as the researcher had not conducted an SLR before, she lacked knowledge on the best practices on how to conduct such a research that can only be accumulated through experience. Additional challenges to the

research was posed by a rigorous work schedule of the researcher that slowed down the thesis process.

The results of the systematic literature review demonstrate that the terminology related to information security services is not well established and leaves room for future research. The incoherent use of terms made it difficult to determine whether the description refers to a service or a function and when terms other than *service* should be included in the research. The use of different terms was largely dependent on the context and, thus, demanded careful consideration of the inclusion or exclusion of these terms. On the other hand, the inclusion of the abstract infosec services – especially CIA – raises concerns on whether the authors possess differing perceptions on the identity of a service itself. Based on the results it is suggested, that the SLR could be extended to cover a broader set of search terms and that future research would aim at finding a categorization between the different terms utilised. It remains unclear, whether a clear division between the different terms can be drawn and whether the authors draw a distinctive line between the various terms. This presents opportunities for an interesting future research.

The systematic literature review evidenced that the list of utilised search terms was not comprehensive as a wide range of other terms was discovered. On the other hand, as the review was only a part of the Master's thesis, some delimiting had to be done. Some prominent terms to include would have been 'cyber security service', 'managed security service', 'information technology service' and 'information system security service'; the two latter were included in the review by using abbreviations 'IT' and 'IS'. However, the use of the term cyber security might obscure the division of information and cyber security further if a clear distinction between the two terms is necessary to maintain. In fact, many of the services themselves could be regarded as cyber security services as they can be utilized in safeguarding more than just the information assets of an organization. The use of the term 'security service' could also be considered as it was present in many articles. However, including the term might pose problems in identifying whether the article refers to information security services or security services in general.

Similarly to the search terms, only a limited amount of six databases was utilized in the systematic literature review. Extending the review to cover more databases would increase the amount of articles and possibly produce more findings. Finding an equilibrium between useful findings, the amount of material to be included and the resources available, though, is a balancing act.

In the future, the time range of the SLR articles to be included could also be limited. This study did not exploit the delimitation of the time range to keep the number of articles sufficient but this was considered as on option during the systematic literature review. The delimitation would be especially useful if a wider range of search terms or databases was utilized. That way the SLR materials could be limited to include only the most recent articles and findings.

The quality of the SLR articles sets another limitation to the study. As noted earlier, most of the articles had a low or non-existent JUFO ranking. Therefore it must be stated, that there is likely room for improvement in the quality of the articles in the review. Articles and other publications with higher JUFO rankings might present more fruitful material for the research.

The type of the publications included in the research also sets a limitation to the study. All of the publications included in the systematic literature review were recognized as scientific literature and most of them were conference proceedings. By including more books, articles and non-scientific literature, the results of the SLR could have been more comprehensive. As the development of digitalisation and information technology accelerates, the scientific literature may not be able to keep up with the pace and, thus, it may not include the most recent developments in the information security field. Therefore, including non-scientific findings and publications from the business side into the review could yield valuable results. This notion is supported by the findings from the survey conducted to business representatives; additional insights to the topic of infosec services were derived from the survey.

During the systematic literature review, a large amount of articles was excluded from the review as they did not fulfil the initial requirements set in the SLR. However, the articles that discussed the topic could have contributed to the findings of the literature review. This idea is supported by Piper (2013, 4) who notes that it might be better to decide on the exclusion of articles based on the whole article, not just the abstract which might have journal-specific limitations. Yet, it must be stated that the inclusion of additional articles is very laborious as the manual handling and screening of the articles demands lots of time and effort. Nevertheless, this is an option to be explored in the future.

The survey also bore some limitations; these limitations are first mirrored through the low response rate. Although the survey was distributed through various channels and people, it only raised 15 responses. Firstly, the main reason for the low number of responses could be that the survey did not reach the eligible group of respondents – people concerned with or responsible for the information security of an organization. The cause for this could be, that the research was unable to reach the most suitable distribution channels. Secondly, another reason for the low response rate might be that the people responsible for the infosec issues within the organization were unwilling or unauthorized to answer the survey. This notion was supported with the feedback given in the survey that mentioned the restrictions for providing infosec service related information. Moreover, organizations have likely been reluctant to disclose this kind of discrete information that is vital to the protection of the company – especially to parties not well known. Furthermore, the WannaCry ransomware attack, which occurred simultaneously with the survey, may have caused companies to be either extremely careful with disclosing information or oth-

erwise occupied with infosec issues. Thirdly, infosec services may be outsourced especially in smaller companies and, thus, the management of the company does not have sufficient knowledge or understanding on how exactly their infosec issues have been arranged. It is also possible that information security service as a concept is seen as unfamiliar.

Furthermore, other reasons for the low response rate can be identified. As mentioned in section 4.1, the initial idea was to distribute the survey via a large partner company with an extensive contact network that would have enabled contacting a wide sample of companies operating in Finland; however, this proved infeasible. The original plan could have yielded more responses due to the good reputation and contacts of the partner company. Utilizing social media in the distribution of the survey, in turn, can be problematic as the survey is then available to all people and not specifically targeted to the intended sample. This could explain both the high number of views in social media (1331 views) and the rather high number of times the survey was opened but left unanswered (over 130 times). As the questions were somewhat specific, the people opening the survey may have noticed that they do not have sufficient expertise to answer the survey. The inclusion of mandatory and open-ended, descriptive questions may also have lowered the willingness to answer the survey – especially by people working in high and demanding roles with a busy schedule. The unwillingness to answer may have been strengthened by the inclusion of questions measuring two issues; the problem with such questions was acknowledged but they were included to increase the usability and fluency of the survey.

The social media invitation itself was quite welcoming which could also have tempted people to open the survey only to receive more information on the Digiwars programme. Additionally, the survey itself was very traditional which could have reduced the motivation to answer it after the expectations of the social media invitation. Another problem with the use of social media is, that the number of respondents from the same organization cannot be limited and, thus, it is possible that representatives of the same organization have answered the survey and distorted the data. This is a non-desirable result concerning the survey and should be more thoroughly considered in the future. A higher response rate might have been achieved by lengthening the response time. However, this was done once and it did not significantly increase the results. Finally, it might be that some people do not regard the topic as interesting or see the research as bringing value to their organization and, thus, the survey has been left unanswered.

From the perspective of the quality of the data collected in the survey, some notions can also be made. If more responses would have been achieved, the responses included in the survey analysis could have been limited based on the role of the respondent. On the other hand, as employees in small companies bear larger areas of responsibility, this might have omitted some relevant responses. Thus, limiting responses based on the role of the respondent is debatable.

One notable limitation in the survey is that it did not measure the location of the companies. As social media was utilized in the distribution of the survey, these locations may be unevenly distributed referring to selection bias. Additionally, the use of social media may pose the research to voluntary bias as LinkedIn permits anyone with an access to the survey to answer it. Additionally, the use of LinkedIn might favour younger, educated users. This is supported by the recent statistics of Finnish LinkedIn users that state that 52.9% of the users in Finland are, in fact, under 35 years old, although the largest individual user group represents older users (ages 35–54; 40% of Finnish LinkedIn users) (Laine 2017). These facts cause concerns to the reliability and validity of the research. The location question was not included in the survey, however, to minimize the amount of identifiable information and to guarantee the anonymity of the respondents.

Another factor influencing the quality of the survey is the fact that professional translators were not utilized in the survey data analysis phase. This might have enabled a more precise analysis, although the questionnaire was presented to the respondents in its original language in Finnish and, thus, problems materializing due to that could not have occurred. However, specialized IT terms that were translated from English to Finnish in the questionnaire may have caused misinterpretations among the survey respondents. To avoid this, short descriptions of the service categories were provided. Another quality factor influencing the research is that investigator triangulation was not utilized in the data analysis which might have yielded richer and more precise results. However, the use of data triangulation instead has benefited the research. In the future, replacing the survey with interviews might prove fruitful as they enable more in-depth discussions on the topic. On the other hand, finding interviewees for the interviews might prove difficult as it would most probably require personal contacts in advance in order for organizations to be willing to disclose such discrete information. The selection between a survey and interviews was carefully considered during the study process and the conclusion was that a survey would better help in answering the research questions and the assignment given by the client. However, utilizing interviews in the future to deepen the results could be considered.

The building of the information security service categorization also pose some challenges. As mentioned earlier, ISSeCa is only one subjective interpretation of the information security services entity. The networked nature of the services made the building of the categorization difficult. Furthermore, as the topic was new to the researcher and partly very technically-oriented, the construction of the categorization proved cumbersome. Thus, the building of the information security service categorization has been a learning experience into information security. Collaboration and discussions with an expert in the field might have made the thesis process more fluent. Furthermore, an expert could have been asked to evaluate the categorization or to build a categorization of their

own, which could then have been compared to ISSeCa. This type of investigator triangulation would increase the credibility of the categorization and the research in general.

An additional limitation to the categorization is caused by the fact that the identified infosec services were handled as equal in the categorization despite their status or frequency in the literature. Therefore, those services that were described as categories in the articles, were placed under the *Other* main category, instead of nominating them as main categories in the categorization. The hierarchy, in turn, was built based on information obtained from the SLR articles, the ISO 27002 standard and VAHTI infosec area descriptions, information searched from the internet and the researcher's own perception. Perhaps in the future, a more precise hierarchy of the identified services could be built. Furthermore, as discussed earlier in section 3.4.3, the services are interlinked by nature, and thus, their relations could be better depicted in the categorization in the future. This notion is supported by Novak and Cañas (2008, 12) who recommend using cross-links between concepts from different branches to demonstrate the connections of those services. However, one should be selective with the linking of concepts due to the natural connectedness of those concepts.

In addition to the ideas for future research presented above, other broader topics for future research could be considered. A new research avenue could be adopted by focusing on the information security service related competence or infosec service outsourcing; both are topics that were touched upon in the research. In fact, Pelkonen et al. (2016) have studied the cyber competence in Finland and present a concept map that resembles the categorization built in this study regarding cyber security technologies. Outsourcing, in turn, is a timely topic as it was recently reported that due to a neglectful outsourcing contract, the discrete information of the Swedish transport authority – including the driving licence register, secret criminal records of the police and the internal data-communications of various Swedish authorities – were accessible to people to whom a security clearance had not been conducted (Onali 2017). This highlights the fact that companies may not always understand the contents of their outsourcing contracts and may be unable to control the compliance of the provider towards the contract. Therefore, the infosec risks related to information security service outsourcing may prove to be a fruitful research area in the future. Other interesting research directions could include the topic of soft services and their impact on the overall information security of an organization and future security services to tackle new security threats.

## 5.3 Implications for practice

This research provides multiple useful insights for practice. Firstly, the ISSeCa categorization provides a checklist for organizations from which they can either search for individual services or, most importantly, with which they can find ways to build a holistic network of security services. Thus, the categorization helps organizations in discovering whether they have considered all necessary areas of infosec services, or whether there are areas yet to be included in their information security service palette.

Furthermore, the categorization helps organizations in understanding that mere technical solutions are not sufficient but one needs to consider other aspects of information security services as well: physical and soft services, people as part of information security and a holistic perspective in building the information security capabilities of the organization. In addition to understanding the multifaceted nature of infosec services, it is of utmost importance for organizations to engage their staff and other stakeholders to follow and adopt the information security instructions of the organization; without true commitment, all the benefits of security services will not materialize. Consequently, as stated earlier, people pose one of the greatest threats on information security. Therefore, it is a matter that needs to be taken into account by all organizations. The holistic perspective, in turn, provides companies with the understanding that single solutions are not sufficient in ensuring information security. Instead, combinations of security services are needed to answer to the security needs of an organization. These notions are supported by von Solms and von Solms (2004, 372–375) who list the lack of information security awareness among users, lack of understanding information security as a business matter instead of a technical matter and the lack of understanding the fact that information security consists of multiple dimensions as among the ten deadly sins regarding information security management.

It is this understanding that helps organizations build their information security puzzle and fit all the needed pieces of the puzzle together to make it complete. However, complete in this context does not refer to final or static – instead, it refers to the puzzle as fulfilling the current needs of the organization. Yet, the organization has to look out for the future and adjust this palette to those upcoming needs when discovered. This signifies the fact, that information security is constantly evolving based on the needs of the company; if static, it may quickly outdate itself. Thus, organizations have to simultaneously plan and optimize the level of investments in infosec services and prepare themselves for future needs.

The final insight for practice is the inclusion of information security into systems and processes early on. Considering infosec related issues already at the early stages of planning will help in creating a better fit with the processes or systems and information secu-

rity, which, in turn, will lead to more fluent processes and a better functioning organization. Information security and corresponding services is a topic concerning all organizations nowadays – therefore, it is a matter not to be taken too lightly.

## 5.4 Implications for research

In addition to practical implications, the research also presents insights for research. Firstly, the systematic literature review (SLR) offers a glance to the discussion on infosec services in academic literature and provides a comprehensive list of security services identified in it. Additionally, the SLR sheds light on the inconsistencies in the topic and offers various opportunities for future research. Furthermore, the research presents the discrepancies regarding infosec services between business and academia. This study proves that the field of security services is still rather undeveloped and lacks coherence. Researchers agree neither with the definition of infosec services nor with what kind of services exist. Therefore, investigating these topics further in the future is recommended.

Furthermore, the categorization provides an approach to handling the infosec service entity in a logical manner – it presents a graphic way of rationally organizing the network of security services. The ISSeCa categorization provides a starting point both for understanding the infosec service network and for deepening understanding of the dependencies between the services.

The research also offers an initial definition for a security service by combining the findings from academic articles and publications with the insights from business practitioners. However, the description is still very wide and could be capsulized further – another opportunity for future studies.

The initial idea was to research the term ‘information security commodity’ given by the client, but already at very early stages of the systematic literature review it became evident that the term is not widely utilised in academic literature. Therefore, the term was changed to ‘information security service’ as it was thought to provide more comprehensive and intriguing results. Based on the findings of this study, the use of the term ‘information security commodity’ would require consolidation and, therefore, the usage of the term is not recommended.

# 6 CONCLUSIONS

This thesis aims at shedding light on the topic of information security services. It investigates how an information security service can be described and what kind of security services are identified in literature. Furthermore, the thesis presents a categorization of the identified infosec services as an attempt to present the network of security services in a structured manner. Based on the results of the research, a consensus on the definition and types of security services is yet to be achieved. This is due to the fact, that the range of infosec services is wide and multiple perspectives on the services exist. Furthermore, to some extent, academia is still describing infosec services by confidentiality, integrity and availability – similarly to the description of information security itself.

The study also presents the results of a survey conducted in companies operating in Finland. Although the results cannot be generalized to a larger population, they provide insights on the outlook of organizations towards infosec services. In fact, according to the results, the companies regard infosec services as important in ensuring the information security of the organizations and utilize a balanced set of infosec service categories in this endeavour. However, despite the increasing security threats, most companies are not planning to invest more in information security services in the future. This may cause problems in the future if the organizations are not committed to developing their information security service palette. Furthermore, both similarities and differences were identified in the way business described and named security services.

The study concludes that companies should adopt a holistic approach in building their information security service palette, where different services are fitted together like the pieces of a puzzle. This puzzle, however, is not built static but needs to be altered based on the emerging organizational needs. The findings of this study provide a fertile ground for future research in the areas of information security services, such as soft services, outsourcing related security threats and security service related competence. Thus, this study operates as a starting point for future findings in the versatile field of information security services.

# REFERENCES

AbdElnapi, Noha MM. – Omara, Fatma A. – Omran, Nahla F. (2016) A hybrid hashing security algorithm for data storage on cloud computing. *International Journal of Computer Science and Information Security*, Vol. 14 (4), 175–181. <https://doi.org/10.13140/RG.2.1.4103.3844>, retrieved 17.9.2016.

Allen, Julia H. – Gabbard, Derek – May, Christopher J. (2003) *Outsourcing managed security services*. Technical report. Security improvement module, CMU/SEI-SIM-012. Software Engineering Institute, Carnegie Mellon. 1–113. <http://repository.cmu.edu/sei/600/>, retrieved 4.6.2017.

Asgarnezhad, Marzieh – Nasiri, Ramin – Sahebhonar, Saeedreza (2010) Analysis and evaluation of two security services in SOA. *2010 Fifth International Conference on Internet and Web Applications and Services (ICIW)*, Barcelona, Spain, May 9–15, 2010, 562–568. <https://doi.org/10.1109/ICIW.2010.92>, retrieved 9.10.2016.

Bahl, Sanjay – Wali, O.P. (2013) An empirical analysis of perceived significance of information security service quality to predict the organisational performance in software service industry. *CSI Transactions on ICT*, Vol. 1 (3), 221–230. <https://doi.org/10.1007/s40012-013-0020-6>, retrieved 9.10.2016.

Bahl, Sanjay – Wali, O.P. (2014) Perceived significance of information security governance to predict the information security service quality in software service industry: An empirical analysis. *Information Management & Computer Security*, Vol. 22 (1), 2–23. <https://doi.org/10.1108/IMCS-01-2013-0002>, retrieved 9.10.2016.

Bowen, Pauline – Hash, Joan – Wilson, Mark (2006) *Information security handbook: A guide for managers. Recommendations of the National Institute of Standards and Technology.* Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930. <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf>, retrieved 22.2.2017.

Buecker, Axel – Ashley, Paul – Bouyssou, Julien – Gargaro, Gianluca – Muppidi, Sridhar – Neucom, Ray – Readshaw, Neil – Schinke, Gregor (2007) *Understanding SOA security design and implementation*. International Technical Support Organization. IBM. <www.redbooks.ibm.com/redbooks/pdfs/sg247310.pdf>, retrieved 22.2.2017.

*CGI: Kyberturvallisuuden tila suomalaisissa organisaatioissa 2016* (2016) CGI, 1–14. <https://www.cgi.fi/sites/default/files/files_fi/pdf/cgi_kyberturvallisuuden-tila_tutkimuraportti2016.pdf>, retrieved 8.5.2017.

Chappell, Brett L. – Marlow, David T. – Irey IV, Phillip M. – O'Donoghue, Karen (1999) IP security impact on system performance in a distributed real-time environment. *Proceedings of the 20th IEEE Real-Time Systems Symposium*, Phoenix, AZ, USA, December 1–3, 1999, 218–219. <https://doi.org/10.1109/REAL.1999.818846>, retrieved 9.10.2016.

Chang, Chin-Chen – Lee, Wei-Bin (2003) Taiwan: Focus on the information security market. *IT Professional*, Vol. 5 (5), 26–29. <https://doi.org/10.1109/MITP.2003.1235606>, retrieved 9.10.2016.

Choi, Yang-seo – Seo, Dong-il (2005) An analysis of ISPs' role as managed security service providers (MSSPs). *The 7th International Conference on Advanced Communication Technology, 2005, ICACT 2005*, Phoenix Park, South Korea, February 21–23, 2005, 624–626. <https://doi.org/10.1109/ICACT.2005.245948>, retrieved 9.10.2016.

Claassen, G.J. – Kühn, G.J. – Penzhorn, W.T. (1992) Information security services and standards for telecommunications in Africa. *3D Africon Conference, Africon '92 Proceedings*, Ezulwini Valley, Swaziland, September 22–24, 1992, 33–36. <https://doi.org/10.1109/AFRCON.1992.624412>, retrieved 9.10.2016.

Classification of instructions (2017) Ministry of Finance. <https://www.vahtio-hje.fi/web/guest/vahti-ohjeet-by-caterogy>, retrieved 28.6.2017.

Creswell, John W. (2003) *Research design: Qualitative, quantitative, and mixed methods approaches*. 2nd ed. Sage Publications, Inc., Thousand Oaks, California. <https://ucalgary.ca/paed/files/paed/2003_creswell_a-framework-for-design.pdf>, retrieved 30.8.2017.

Creswell, John W. (2010) Mapping the developing landscape of mixed methods research. *SAGE handbook of mixed methods in social & behavioral research*, 2nd ed., eds. Tashakkori, Abbas – Teddlie, Charles, 45–68. SAGE Publications, Inc., Thousand Oaks, California. <http://dx.doi.org/10.4135/9781506335193.n2>, retrieved 16.6.2016.

Creswell, John W. – Plano Clark, Vicky L. (2007) *Designing and conducting mixed methods research*. Sage Publications, Inc., Thousand Oaks, California. <https://books.google.fi/books/about/Designing_and_Conducting_Mixed_Methods_R.html?id=FnY0BV-q-hYC&redir_esc=y>, retrieved 16.6.2016.

Crotty, Michael (1998) *The foundations of social research: Meaning and perspective in the research process*. Sage Publications Ltd, London. <https://books.google.fi/books?id=fEpOCgAAQBAJ&hl=fi>, retrieved 30.8.2017.

Datta Ray, Partha – Harnoor, Rajgopal – Hentea, Mariana (2010) Smart power grid security: A unified risk management approach. *44th Annual 2010 IEEE International Carnahan Conference on Security Technology (ICCST)*, San Jose, CA, USA, October 5–8, 2010, 276–285. <https://doi.org/10.1109/CCST.2010.5678681>, retrieved 9.10.2016.

Deng, Robert H. – Bhonsle, Shailendra K. – Wang, Weiguo – Lazar, Aurel A. (1995) Integrating security in CORBA based object architectures. *Proceedings of the 1995 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, May 8–10, 1995, 50–61. <http://doi.org/10.1109/SECPRI.1995.398922>, retrieved 9.10.2016.

Denzin, Norman K. (2009) *The research act: A theoretical introduction to sociological methods*. AldineTransaction, Transaction Publishers, New Brunswick. <https://books.google.fi/books?id=UjcpxFE0T4cC&hl=fi>, retrieved 7.8.2017.

Digiwars - keeping the Force (2017) Tietokayttoon.fi. Valtioneuvoston selvitys- ja tutkimustoiminta. Prime Minister's Office. <http://tietokayttoon.fi/hankkeet/hanke-esittely/-/asset_publisher/digiwars-keeping-the-force>, retrieved 7.3.2017.

*Effective information security* (2009) A summary of general instructions on information security management. The Government Information Security Management Board, VAHTI, Ministry of Finance, 5/2009, 1–88. Edita Prima Plc, Helsinki. <https://www.vahtiohje.fi/web/guest/5/2009-effective-information-security>, retrieved 2.8.2016.

ENISA (2006) *Risk Management: Implementation principles and inventories for risk management / Risk assessment methods and tools*. ENISA – European Network and Information Security Agency. Technical Department, Section Risk Management, June 2006, 1–177. <https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools>, retrieved 24.7.2016.

Eriksson, Päivi – Kovalainen, Anne (2008) Chapter 4: Focus on frame. *Qualitative methods in business research*. SAGE Publications Ltd, London. <http://dx.doi.org/10.4135/9780857028044.d24>, retrieved 4.6.2017.

*EU-tietosuojan kokonaisuudistus* (2016) VAHTI-raportti – 1/2016. Julkisen hallinnon ICT. Valtiovarainministeriö. <https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128>, retrieved 19.9.2017.

Evaluations (2017) Publication Forum. Federation of Finnish Learned Societies. <http://julkaisufoorumi.fi/en/evaluations>, retrieved 26.6.2017.

Feng, Jun – Chen, Yu – Ku, Wei-Shinn – Liu, Pu (2010) Analysis of integrity vulnerabilities and a non-repudiation protocol for cloud data storage platforms. *ICPPW '10 Proceedings of the 2010 39th International Conference on Parallel Processing Workshops*, San Diego, California, USA, September 13–16, 2010, 251–258. <https://doi.org/10.1109/ICPPW.2010.42>, retrieved 1.8.2017.

Greene, Jennifer C. (2008) Is mixed methods social inquiry a distinctive methodology? *Journal of Mixed Methods Research*, Vol. 2 (1), 7–22. <https://doi.org/10.1177/1558689807309969>, retrieved 31.8.2017.

Hakala, Juha T. (2005) *Graduopas. Melkein maisterin niksikirja*. GAUDEAMUS, Oy Yliopistokustannus University Press Finland Ltd., Helsinki.

Hakala, Mika – Vainio, Mika – Vuorinen, Olli (2006) *Tietoturvallisuuden käsikirja*. Docendo Finland Oy, Jyväskylä.

Halminen, Laura (2014) Tutkimus: Lähes puolet suomalaisyritysten tietoverkoista saastuneita. *Helsingin Sanomat*, 15.1.2014. <http://www.hs.fi/kotimaa/a1389777593822>, retrieved 5.6.2016.

Hartikainen, Jarno (2016) Sakonuhka patistaa ryhtiliikkeeseen tietoturvassa. *Kauppalehti* 17.3.2016. <http://www.kauppalehti.fi/uutiset/sakonuhka-patistaa-ryhtiliikkeeseen-tietoturvassa/Tvg47xD3>, retrieved 5.6.2016.

Heikkilä, Tarja (2008) *Tilastollinen tutkimus*. 7th revised ed. Edita Publishing Oy, Helsinki.

Hirsjärvi, Sirkka – Remes, Pirkko – Sajavaara, Paula (2003) *Tutki ja kirjoita*. 6th – 9th ed. Kustannusosakeyhtiö Tammi, Helsinki.

Home (2017) Publication Forum. Federation of Finnish Learned Societies. <http://julkaisufoorumi.fi/en>, retrieved 26.6.2017.

ICT-Portti (2017) ICT-portti. <http://www.ictportti.fi/?page_id=214>, retrieved 12.12.2017.

Inductive Approach (Inductive Reasoning) (2016) Research Methodology. Necessary knowledge to conduct a business research. <http://research-methodology.net/research-methodology/research-approach/inductive-approach-2/>, retrieved 19.6.2016.

Irvine, Cynthia – Levin, Timothy (2000) Quality of security service. *NSPW '00 Proceedings of the 2000 workshop on New security paradigms*, Ballycotton, County Cork, Ireland, September 18–21, 2000, 91–99. <https://doi.org/10.1145/366173.366195>, retrieved 13.6.2017.

ISO/IEC 27002 (2013) *Information technology – Security techniques – Code of practice for information security controls*. International standard. 2nd ed.

Jeong, Chang Won – Joo, Su Chong – Jeong, Young Sik (2010) Mobile collaboration environment based on distributed object group framework for u-hospital. *2010 Proceedings of the 5th International Conference on Ubiquitous Information Technologies and Applications (CUTE)*, December 16–18, 2010, Sanya, China, 1–5. <https://doi.org/10.1109/ICUT.2010.5677641>, retrieved 9.10.2016.

Jin, Seunghun – Cho, Sangrae – Choi, Daeseon – Ryou, Jae-Cheol (2003) New security paradigm for application security infrastructure. *Information networking. ICOIN 2003. Lecture notes in computer science,* Vol. 2662, ed. Kahng, Hyun-Kook, 793–802. Springer-Verlag Berlin Heidelberg. <http://doi.org/10.1007/978-3-540-45235-5_78>, retrieved 9.10.2016.

Johnson, R. Burke – Onwuegbuzie, Anthony J. (2004) Mixed methods research: A research paradigm whose time has come. *Educational Researcher*, Vol. 33, (7), 14–26. <http://dx.doi.org/10.3102/0013189X033007014>, retrieved 20.6.2016.

Jøsang, Audun – Ismail, Roslan – Boyd, Colin (2007) A survey of trust and reputation systems for online service provision. *Decision Support Systems*, Vol. 43 (2), 618–644. <https://doi.org/10.1016/j.dss.2005.05.019>, retrieved 23.5.2017.

Kananen, Jorma (2008) *KVANTTI. Kvantitatiivinen tutkimus alusta loppuun*. Jyväskylän ammattikorkeakoulun julkaisuja -sarja, ed. Ijäs, Eva. Jyväskylän ammattikorkeakoulu, Jyväskylä.

Karokola, Geoffrey – Kowalski, Stewart – Yngström, Louise (2011a) Secure e-government services: Towards a framework for integrating IT security services into e-government maturity models. *2011 Information Security for South Africa (ISSA)*, Johannesburg, South Africa, August 15–17, 2011, 1–9. <https://doi.org/10.1109/ISSA.2011.6027525>, retrieved 9.10.2016.

Karokola, G. – Kowalski, S. – Yngström, L. (2011b) Towards an information security maturity model for secure e-government services: A stakeholders view. *Proceedings of the Fifth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2011)*, July 7–8, 2011, London, United Kingdom, eds. Furnell, Steven – Clarke, Nathan, 58–73. <https://books.google.fi/books?id=3apGAwAAQBAJ&dq=%22Proceedings+of+the+Fifth+International+Symposium+on+Human+Aspects+of%22&hl=fi>, retrieved 31.1.2017.

Karokola, Geoffrey – Kowalski, Stewart – Yngström, Louise (2013) Evaluating a framework for securing e-government services – A case of Tanzania. *2013 46th Hawaii International Conference on System Sciences (HICSS)*, Wailea, Maui, HI, USA, January 7–10, 2013, 1792–1801. <https://doi.org/10.1109/HICSS.2013.208>, retrieved 9.10.2016.

Karyda, Maria – Mitrou, Evangelia – Quirchmayr, Gerald (2006) A framework for outsourcing IS/IT security services. *Information Management & Computer Security*, Vol. 14 (5), 403–416. <https://doi.org/10.1108/09685220610707421>, retrieved 9.10.2016.

Keeratiwintakorn, Phongsak – Krishnamurthy, Prashant (2006) Energy efficient security services for limited wireless devices. *2006 1st International Symposium on Wireless Pervasive Computing*, Phuket, Thailand, January 16–18, 2006, 1–6. <https://doi.org/10.1109/ISWPC.2006.1613636>, retrieved 9.10.2016.

Kitchenham, Barbara – Charters, Stuart (2007) *Guidelines for performing systematic literature reviews in software engineering*. EBSE technical report, EBSE-2007-01. Version 2.3, July 9, 2007, 1–57. <https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf>, retrieved 21.08.2016.

Kotler, Philip – Keller, Kevin Lane (2011) *Marketing Management*. 14th ed. Prentice Hall, Upper Saddle River, New Jersey. <http://socioline.ru/files/5/283/kotler_keller_-_marketing_management_14th_edition.pdf>, retrieved 3.5.2017.

Kovač, Damjan – Trček, Denis (2009) Qualitative trust modeling in SOA. *Journal of Systems Architecture*, Vol. 55 (4), 255–263. <http://doi.org/10.1016/j.sysarc.2009.01.002>, retrieved 9.10.2016.

Laine, Tom (2017) Suomalaiset Linkedinissä - uusia tilastoja, kesäkuu 2017. HC Services Oy, 29.6.2017. <https://www.somehow.fi/suomalaiset-linkedinissa-uusia-tilastoja-kesakuu-2017/>, retrieved 19.9.2017.

Lee, Wongoo – Kim, Sijung – Kim, Bonghan (2006) Response against hacking and malicious code in P2P. *Computational Science and Its Applications - ICCSA 2006. ICCSA 2006, Lecture notes in computer science*, Vol. 3984, eds. Gavrilova, Marina L. – Gervasi, Osvaldo – Kumar, Vipin – Tan, C. J. Kenneth – Taniar, David – Laganá, Antonio – Mun, Youngsong – Choo, Hyunseung, 851–857. Springer-Verlag Berlin Heidelberg. <http://doi.org/10.1007/11751649_93>, retrieved 9.10.2016.

Levitt, Theodore (1981) Marketing intangible products and product intangibles. *Cornell Hospitality Quarterly*, Vol. 22 (2), 37–44. <https://doi.org/10.1177/001088048102200209>, retrieved 8.5.2017.

Lin, Zhang – Zhixin, Chen (2010) Design and implementation of a e-commerce system based on PKI. *2010 International Conference on Computer and Communication Technologies in Agriculture Engineering (CCTAE)*, Chengdu, China, June 12–13, 2010, 4–7. <https://doi.org/10.1109/CCTAE.2010.5543753>, retrieved 9.10.2016.

Linnake, Tuomas (2017) Yahoo-pomo myöntää hakkerimokan: Luopuu miljoonistaan. *Digitoday*, 2.3.2017. <http://www.is.fi/digitoday/tietoturva/art-2000005111088.html>, retrieved 7.3.2017.

Liping, Hou – Lei, Shi (2011) Research on trust model of PKI. *2011 Fourth International Conference on Intelligent Computation Technology and Automation (ICICTA)*, Shenzhen, Guangdong, China, March 28–29, 2011, 232–235. <https://doi.org/10.1109/ICICTA.2011.67>, retrieved 9.10.2016.

Lu, Wenhai – Liu, Shuming – Yang, Yi – Fu, Ruiquan – Xiang, Xianquan – Qu, Yanmin – Huang, Haiyan (2015) Design for the emergency command information system architecture of ocean oil spill. *Aquatic Procedia*, Vol. 3, 41–49. <https://doi.org/10.1016/j.aqpro.2015.02.226>, retrieved 9.10.2016.

Machi, Lawrence A. – McEvoy, Brenda T. (2009) *The literature review: Six steps to success*. Corwin Press, Thousand Oaks, California. <https://books.google.fi/books?id=xPCVe-xuhZcC&dq=Machi+%26+McEvoy+(2008)+%22The+Literature+Review:+Six+Steps+to+Success%22+google+books&hl=fi>, retrieved 23.11.2017.

Manen, Max van (2016) *Researching lived experience: Human science for an action sensitive pedagogy*. 2nd ed. Routledge, Abingdon, Oxon. <https://books.google.fi/books?id=1LZmDAAAQBAJ&dq=Van+Manen,+M.+(1990).+Researching+lived+experience:+Human+science+for+an+action+sensitive+pedagogy&lr=&hl=fi>, retrieved 29.8.2017.

Miguel, Jorge – Caballé, Santi – Xhafa, Fatos – Snasel, Vaclav (2015) A data visualization approach for trustworthiness in social networks for on-line learning. *2015 IEEE 29th International Conference on Advanced Information Networking and Applications (AINA)*, Gwangiu, South Korea, March 24–27, 2015, 490–497. <https://doi.org/10.1109/AINA.2015.226>, retrieved 9.10.2016.

Mikroyritys (2017) Tilastokeskus. <http://www.stat.fi/meta/kas/mikroyritys.html>, retrieved 8.5.2017.

Ministeriöiden verkkopalveluihin hyökättiin jälleen (2016) *Digitoday*, 11.5.2016. <http://www.is.fi/digitoday/tietoturva/art-2000001911084.html>, retrieved 7.3.2017.

Ministry of Transport and Communications (2015) Suomesta suotuisa toimintaympäristö digitaaliselle liiketoiminnalle. Finnish Government. 1.9.2015. <http://valtioneuvosto.fi/artikkeli/-/asset_publisher/suomesta-suotuisa-toimintaymparisto-digitaaliselle-liiketoiminnalle>, retrieved 14.9.2017.

Morgan, Steve C. (2017) *Cybersecurity Market Report*. Cybersecurity Ventures. <http://cybersecurityventures.com/cybersecurity-market-report/>, retrieved 1.10.2017.

Moulton, Rolf – Coles, Robert S. (2003) A contest to evaluate IT security services management. *Computers & Security*, Vol. 22 (3), 204–206. <http://doi.org/10.1016/S0167-4048(03)00306-7>, retrieved 9.10.2016.

Ng, Alfred (2017) The global ransomware epidemic is just getting started. *CNET Magazine*, CBS Interactive Inc. 28.6.2017. <https://www.cnet.com/news/petya-goldeneye-wannacry-ransomware-global-epidemic-just-started/>, retrieved 4.8.2017.

Novak, Joseph D. – Cañas, Alberto J. (2008) The theory underlying concept maps and how to construct and use them. Technical report IHMC CmapTools 2006-01, revised 2008-01, 1–36. <http://cmap.ihmc.us/docs/pdf/TheoryUnderlyingConceptMaps.pdf>, retrieved 23.11.2017.

Oladapo, Samuel – Zavarsky, Pavol – Ruhl, Ron – Lindskog, Dale – Igonor, Andy (2009) Managing risk of IT security outsourcing in the decision-making stage. *2009 International Conference on Computational Science and Engineering, CSE '09*, Vancouver, BC, Canada, August 29–31, 2009, 456–461. <https://doi.org/10.1109/CSE.2009.95>, retrieved 9.10.2016.

Onali, Alma (2017) Tietoturvaskandaali ravistelee Ruotsia – suomalainen asiantuntija pitää tapausta hyvänä muistutuksena ulkoistamisen riskeistä. *Helsingin Sanomat* 24.7.2017. <http://www.hs.fi/ulkomaat/art-2000005301786.html>, retrieved 25.7.2017.

Orlikowski, Wanda J. – Baroudi, Jack J. (1991) Studying information technology in organizations: Research approaches and assumptions. *Information Systems Research*, Vol. 2, (1), 1–28. The Institute of Management Sciences. <http://citeseer.ist.psu.edu/viewdoc/download;jsessionid=E3C329A21C5D6E0C296923404E80323C?doi=10.1.1.103.107&rep=rep1&type=pdf>, retrieved 19.6.2016.

*Path to cyber resilience: Sense, resist, react* (2016) EY's 19th Global Information Security Survey 2016–17. Ernst & Young, 1–26. <http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2016-pdf/%24FILE/GISS_2016_Report_Final.pdf>, retrieved 14.11.12017.

Peiris, Hasala – Soysa, Lakshan – Palliyaguru, Rohana (2008) Non-repudiation framework for e-government applications. *2008 4th International Conference on Information and Automation for Sustainability, ICIAFS 2008*, Colombo, Sri Lanka, December 12–14, 2008, 307–313. <https://doi.org/10.1109/ICIAFS.2008.4783950>, retrieved 9.10.2016.

Pelkonen, Antti – Ahlqvist, Toni – Leinonen, Anna – Nieminen, Mika – Salonen, Jarno – Savola, Reijo – Savolainen, Pekka – Suominen, Arho – Toivanen, Hannes – Kyheröinen, Jukka – Remes, Juha (2016) *Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen*. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2016, February 2016, 1–90. <http://tietokayttoon.fi/julkaisu?pubid=9301>, retrieved 4.8.2017.

Pienet ja keskisuuret yritykset (2017) Tilastokeskus. <http://www.stat.fi/meta/kas/pienet_ja_keski.html>, retrieved 8.5.2017.

Piper, Rory J. (2013) *How to write a systematic literature review: A guide for medical students*. University of Edinburgh. National AMR – Fostering Medical Research.<http://cures.cardiff.ac.uk/files/2014/10/NSAMR-Systematic-Review.pdf>, retrieved 20.4.2017.

Potlapally, Nachiketh R. – Ravi, Srivaths – Raghunathan, Anand – Jha, Niraj K. (2006) A study of the energy consumption characteristics of cryptographic algorithms and security protocols. *IEEE Transactions on Mobile Computing*, Vol. 5 (2), 128–143. <https://doi.org/10.1109/TMC.2006.16>, retrieved 6.6.2017.

Priescu, Iustin – Patriciu, Victor Valeriu – Nicolaescu, Sebastian (2009) The viewpoint of e-commerce security in the digital economy. *2009 International Conference on Future Computer and Communication, ICFCC 2009*, Kuala Lumpur, Malaysia, April 3–5, 2009, 431–433. <https://doi.org/10.1109/ICFCC.2009.43>, retrieved 9.10.2016.

Rachedi, Abderrezak – Benslimane, Abderrahim (2016) Multi-objective optimization for security and QoS adaptation in wireless sensor networks. *2016 IEEE International Conference on Communications (ICC)*, Kuala Lumpur, Malaysia, May 22–27, 2016, 1–7. <https://doi.org/10.1109/ICC.2016.7510879>, retrieved 9.10.2016.

Ransomware cyber-attack: Who has been hardest hit? (2017) *BBC News Services*, BBC 15.5.2017. <http://www.bbc.com/news/world-39919249>, retrieved 4.8.2017.

Rasmusson, Lars – Jansson, Sverker (1996) Simulated social control for secure internet commerce. *NSPW '96 Proceedings of the 1996 workshop on New security paradigms*, Lake Arrowhead, California, USA, September 17–20, 1996, 18–25. <https://doi.org/10.1145/304851.304857>, retrieved 5.6.2017.

*Responsible conduct of research and procedures for handling allegations of misconduct in Finland* (2012) Finnish Advisory Board on Research Integrity (TENK). <http://www.tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf>, retrieved 7.8.2017.

Rissanen, Juha – Koivuranta, Esa (2016) Verkkorikolliset tunkeutuvat sairaalan verkkoon, lukitsevat tiedostoja ja vaativat rahaa – Ovatko tietoni turvassa? *Yle* 29.5.2016. <https://yle.fi/uutiset/3-8904018>, retrieved 3.10.2017.

Rousku, Kimmo (2014) *Kyberturvaopas – Tietoturvaa kotona ja työpaikalla*. Talentum Media Oy, Helsinki.

Schultz, E. Eugene (1995) A new perspective on firewalls. *Network Security*, Vol. 1995 (10), 13–17. <http://doi.org/10.1016/1353-4858(96)89760-1>, retrieved 9.10.2016.

SFS (2012) *SFS-käsikirja 327. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Information technology. Security techniques. Information security management systems*. Suomen Standardoimisliitto SFS ry, Helsinki.

Shaikh, Riaz A. – Sharif, Kashif – Ahmed, Ejaz (2005) Performance analysis of unified enterprise application security framework. *2005 Student Conference on Engineering Sciences and Technology, (SCONEST 2005)*, August 27, 2005, Karachi, Pakistan, 1–7. <https://doi.org/10.1109/SCONEST.2005.4382878>, retrieved 9.10.2016.

Sidiroglou, Stelios – Stavrou, Angelos – Keromytis, Angelos D. (2007) Mediated overlay services (MOSES): Network security as a composable service. *2007 IEEE Sarnoff Symposium*, April 30 – May 2, 2007, Princeton, NJ, USA, 1–7. <https://doi.org/10.1109/SARNOF.2007.4567338>, retrieved 9.10.2016.

Siekkinen, Pertti (1997) Käsitekartan tekemisestä ja sen tietokonesovelluksista. Jyväskylän yliopisto, TITU/Koulutusteknologiakeskus. <http://matriisi.ee.tut.fi/kamu/julkaisut/raportit/pertti_co/kasiteweb.html>, retrieved 22.11.2017.

Siponen, Mikko T. – Oinas-Kukkonen, Harri (2007) A review of information security issues and respective research contributions. *ACM SIGMIS Database: The DATA BASE for Advances in Information Systems*, Vol. 38 (1), 60–80. <https://doi.org/10.1145/1216218.1216224>, retrieved 10.7.2016.

Smith, Jeff H. – Dinev, Tamara – Xu, Heng (2011) Information privacy research: An interdisciplinary review. *MIS Quarterly*. Vol. 35 (4), 989-1015. <https://www.researchgate.net/publication/220260183_Information_Privacy_Research_An_Interdisciplinary_Review>, retrieved 12.9.2017.

Solms, Basie von – Solms, Rossouw, von (2004) The 10 deadly sins of information security management. *Computers & Security*, Vol. 23 (5), 371–376. <https://doi.org/10.1016/j.cose.2004.05.002>, retrieved 14.8.2017.

Solms, Rossouw von – Niekerk, Johan van (2013) From information security to cyber security. *Computers & Security*, Vol. 38, (2013) 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>, retrieved 13.8.2017.

Soomro, Zahoor Ahmed – Shah, Mahmood Hussain – Ahmed, Javed (2016) Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, Vol. 36 (2), 215–225. <https://doi.org/10.1016/j.ijinfomgt.2015.11.009>, retrieved 19.9.2017.

Strauss, Anselm L. – Corbin, Juliet M. (1998) *Basics of qualitative research: Techniques and procedures for developing grounded theory*. 2nd ed. SAGE Publications, Inc.; Thousand Oaks, California. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.461.6630&rep=rep1&type=pdf>, retrieved 11.5.2017.

Sun, Jianguang – Chen, Yan (2008) Intelligent enterprise information security architecture based on service oriented architecture. *2008 International Seminar on Future Information Technology and Management Engineering, FITME '08*, November 20, 2008, Leicestershire, United Kingdom, 196–200. <https://doi.org/10.1109/FITME.2008.30>, retrieved 9.10.2016.

Tamilarasan, A. – Shankarapani, M. K. – Qin, X. – Mukkamala, S. – Sung, A. H. (2008) Integrating energy efficiency and security for storage systems. *2008 IEEE International Conference on Systems, Man and Cybernetics, SMC 2008*, October 12–15, 2008, Singapore, Singapore, 2396–2400. <https://doi.org/10.1109/ICSMC.2008.4811653>, retrieved 9.10.2016.

Tieteenfilosofiset suuntaukset (2015) University of Jyväskylä. <https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tieteenfilosofiset-suuntaukset/tieteenfilosofiset-suuntaukset?set_language=fi&cl=fi>, retrieved 19.6.2016.

*Toimintasuunnitelma strategisen hallitusohjelman kärkihankkeiden ja reformien toimeenpanemiseksi 2015–2019* (2016) Päivitys 2016. Hallituksen julkaisusarja 2/2016. Valtioneuvoston kanslia, Helsinki, 1–90. <http://valtioneuvosto.fi/documents/10184/321857/Toimintasuunnitelma+strategisen+hallitusohjelman+k%C3%A4rkihankkeiden+ja+reformien+toimeenpanemiseksi+2015%E2%80%932019%2C+p%C3%A4ivitys+2016/305dcb6c-c9f8-4aca-bbbb-1018cd7a1fd8>, retrieved 15.9.2017.

Tonge, Atul M. – Kasture, Suraj S. – Chaudhari, Surbhi R. (2013) Cyber security: Challenges for society - literature review. *IOSR Journal of Computer Engineering (IOSR-JCE)*, Vol. 12 (2), 67–75. <http://www.iosrjournals.org/iosr-jce/papers/Vol12-issue2/K01226775.pdf?id=15>, retrieved 10.7.2016.

Trochim, William M. – Donnelly, James P. – Arora, Kanika (2016) *Research methods: The essential knowledge base*. 2nd ed. Cengage Learning, Boston, MA. <https://books.google.fi/books?id=0yxB-BAAAQBAJ&dq=Trochim,+W.+(2000).+The+Research+Methods+Knowledge+Base,+2nd+Edition&hl=fi>, retrieved 14.12.2017.

VAHTI-toiminta (2017) Valtiovarainministeriö. <http://vm.fi/vahti>, retrieved 16.8.2017.

*Valtionhallinnon tietoturvakäsitteistö* (2003) Valtiovarainministeriö, Hallinnon kehittämisosasto, VAHTI, 4/2003, 1–107. Edita Prima Oy, Helsinki. <https://www.yumpu.com/fi/document/view/8316870/valtionhallinnon-tietoturvakasitteisto-valtiovarainministerio>, retrieved 16.8.2017.

*Valtionhallinnon tietoturvasanasto* (2008) Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI, Valtiovarainministeriö, 8/2008, 1–187. Edita Prima Oy, Helsinki. <https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto>, retrieved 10.7.2016.

Vargo, Stephen L. – Lusch, Robert F. (2004) Evolving to a new dominant logic for marketing. *Journal of Marketing*, Vol. 68 (1), 1–17. <http://www.jstor.org/stable/30161971>, retrieved 21.8.2017.

Vilkka, Hanna (2015) *Tutki ja kehitä*. 4th revised ed. PS-kustannus, Jyväskylä.

Virtanen, Jori (2017) Näin toimii WannaCry-haittaohjelma – ”Uudet hyökkäykset ovat väistämättömiä". *Tivi,* Alma Media Oyj 15.5.2017. <http://www.tivi.fi/Kaikki_uutiset/nain-toimii-wannacry-haittaohjelma-uudet-hyokkaykset-ovat-vaistamattomia-6649236>, retrieved 4.8.2017.

Vorakulpipat, Chalee – Siwamogsatham, Siwaruk – Kawtrakul, Asanee (2014) An investigation of information security as a service practice: Case study in healthcare. *International Journal of Computer Applications in Technology*, Vol. 49 (3/4), 365–371. <https://doi.org/10.1504/IJCAT.2014.062372>, retrieved 9.10.2016.

Wahab, Abdi – Bahaweres, Rizal Broer – Alaydrus, Mudrik – Muhaemin – Sarno, Riyanarto (2013) Performance analysis of VoIP client with integrated encryption module. *2013 1st International Conference on Communications, Signal Processing, and Their Applications, (ICCSPA)*; February 12–14, 2013, Sharjah, United Arab Emirates, 1–6. <https://doi.org/10.1109/ICCSPA.2013.6487300>, retrieved 26.11.2016.

Wang, Yanliang – Deng, Song – Lin, Wei-Min – Zhang, Tao – Yu, Yong (2010) Research of electric power information security protection on cloud security. *2010 International Conference on Power System Technology (POWERCON)*, October 24–28, 2010, Hangzhou, China, 1–6. <https://doi.org/10.1109/POWERCON.2010.5666728>, retrieved 9.10.2016.

Weber, Ron (2004) Editor's comments. The rhetoric of positivism versus interpretivism: A personal view. *MIS Quarterly*, Vol. 28 (1), 1–10. <http://www.misq.org/misq/downloads/download/editorial/25/>, retrieved 19.6.2016.

Whitman, Michael E. – Mattord, Herbert J. (2012) *Principles of information security*, 4th ed. Course Technology, Cengage Learning, Boston, MA. <https://books.google.fi/books?id=L3LtJAxcsmMC&dq=soft+security+physical+nformation+security&lr=&hl=fi>, retrieved 26.4.2017.

Wirtz, Jochen – Lovelock, Christopher H. (2016) *Services marketing: People, technology, strategy*. 8th ed. World Scientific Publishing Co. Inc., Hackensack, NJ. <https://books.google.fi/books/about/Services_Marketing.html?id=dKJIDQAAQBAJ&source=kp_cover&redir_esc=y&hl=fi>, retrieved 3.5.2017.

Xia, ZhengYou – Hu, YunAn (2006) Extending RSVP for quality of security service. *IEEE Internet Computing*, Vol. 10 (2), 51–57. <https://doi.org/10.1109/MIC.2006.27>, retrieved 9.10.2016.

Yahoolta uusi paljastus: yli miljardi käyttäjätiliä hakkeroitu – myös Valkoisen talon väkeä (2016) *Taloussanomat–Bloomberg* 15.12.2016. <http://www.is.fi/taloussanomat/art-2000005007551.html>, retrieved 7.3.2017.

Yamany, Hany F. El – Capretz, Miriam A. M. (2008) Use of data mining to enhance security for SOA. *2008 Third International Conference on Convergence and Hybrid Information Technology, ICCIT '08,* November 11–13, 2008, Busan, South Korea, 551–558. <https://doi.org/10.1109/ICCIT.2008.173>, retrieved 9.10.2016.

Yin, Robert K. (2011) *Qualitative research from start to finish*. The Guilford Press, New York, NY. <http://soh.iums.ac.ir/uploads/32_282_77_16.pdf>, retrieved 11.5.2017.

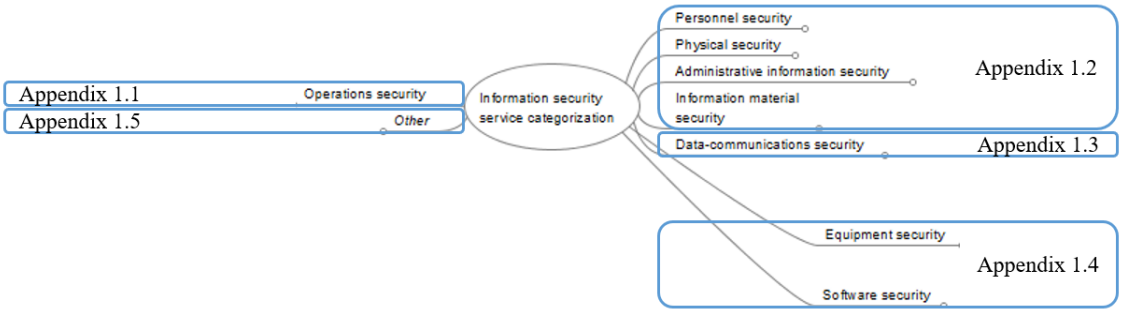
Zhou, Jianying – Gollmann, Dieter (1997) Evidence and non-repudiation. *Journal of Network and Computer Applications*, Vol. 20 (3), 267–281. <https://doi.org/10.1006/jnca.1997.0056>, retrieved 6.6.2017.

Zissis, Dimitrios – Lekkas, Dimitrios (2012) Addressing cloud computing security issues. *Future Generation Computer Systems*, Vol. 28 (3), 583–592. <https://doi.org/10.1016/j.future.2010.12.006>, retrieved 6.6.2017.

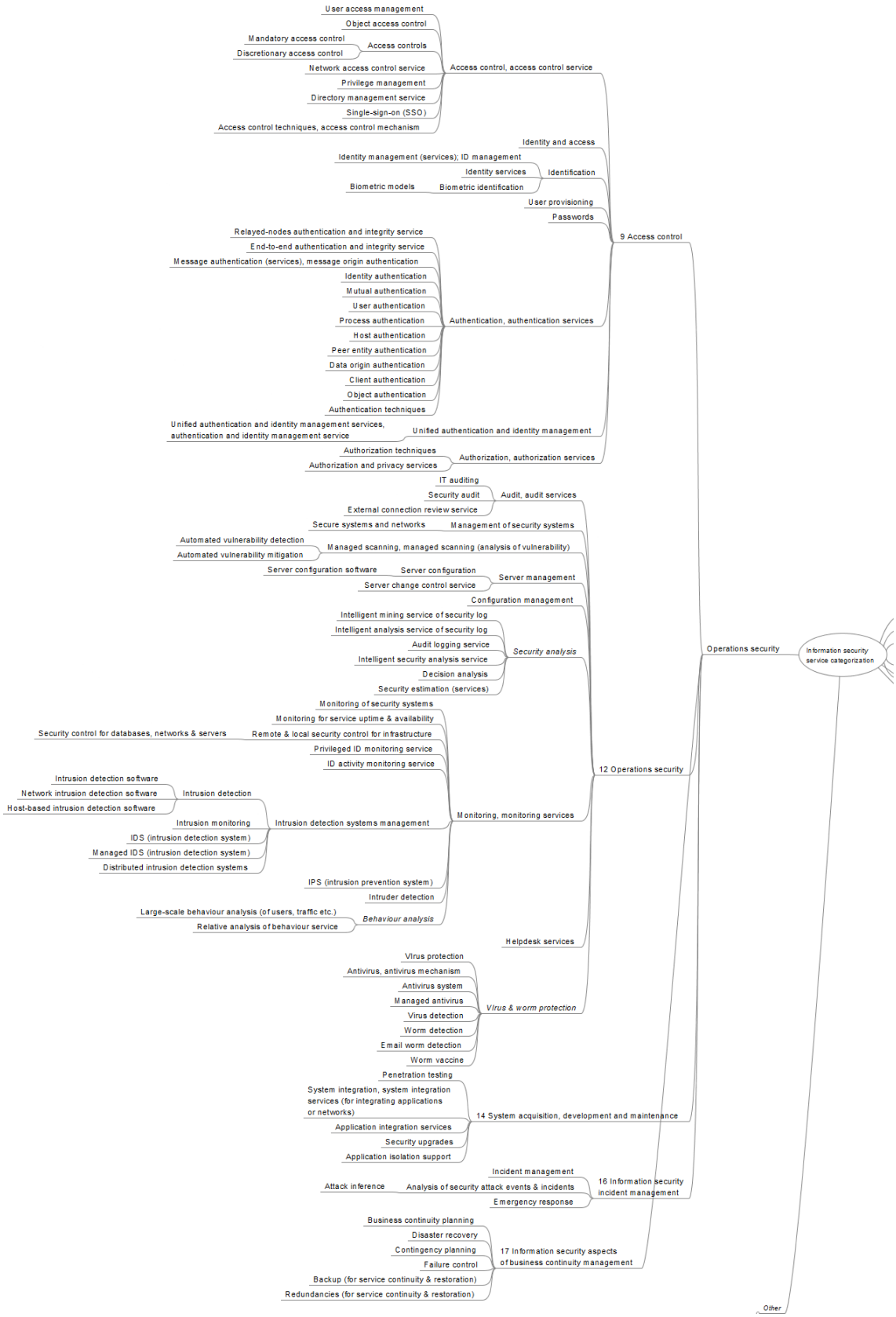
# APPENDICES

APPENDIX 1.0 ISSeCa information security categorization

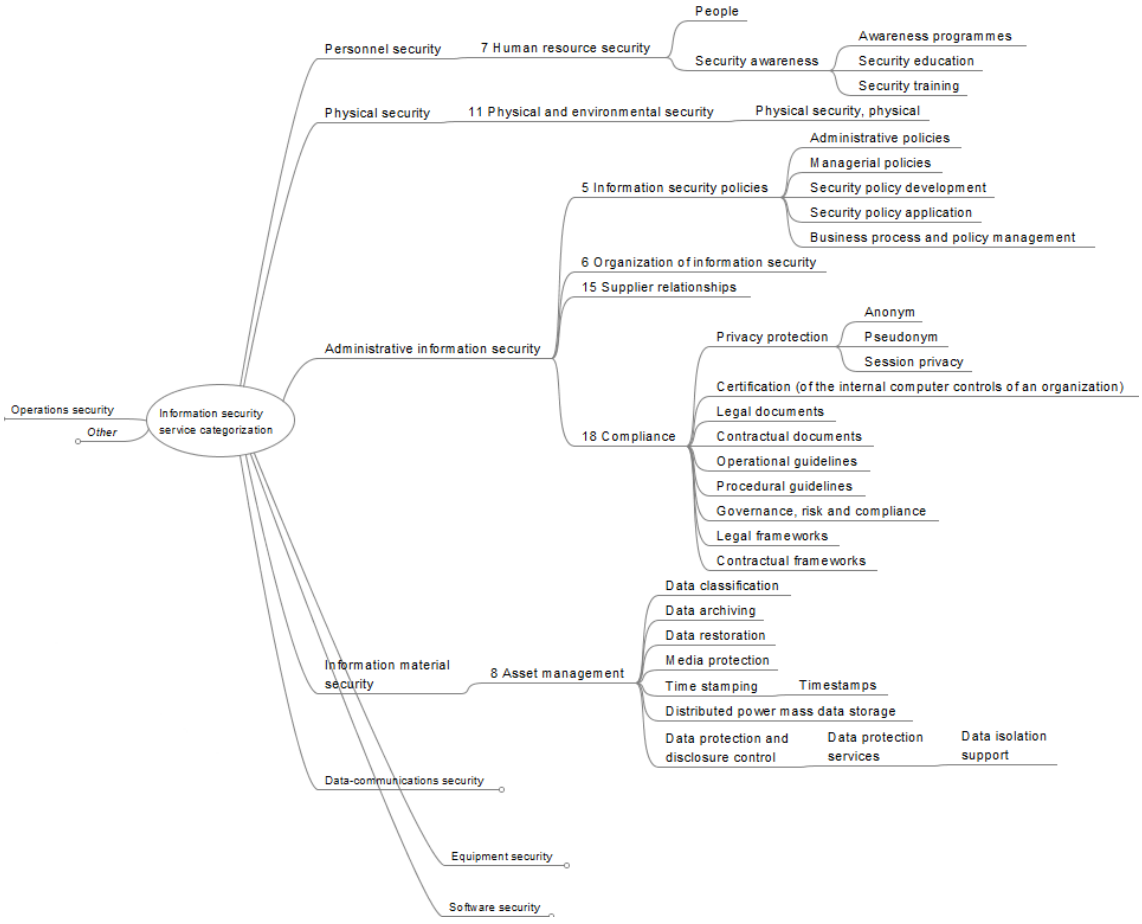
Terms in *italics* are not information security services identified during the systematic literature review but additions to support the structure of the categorization.



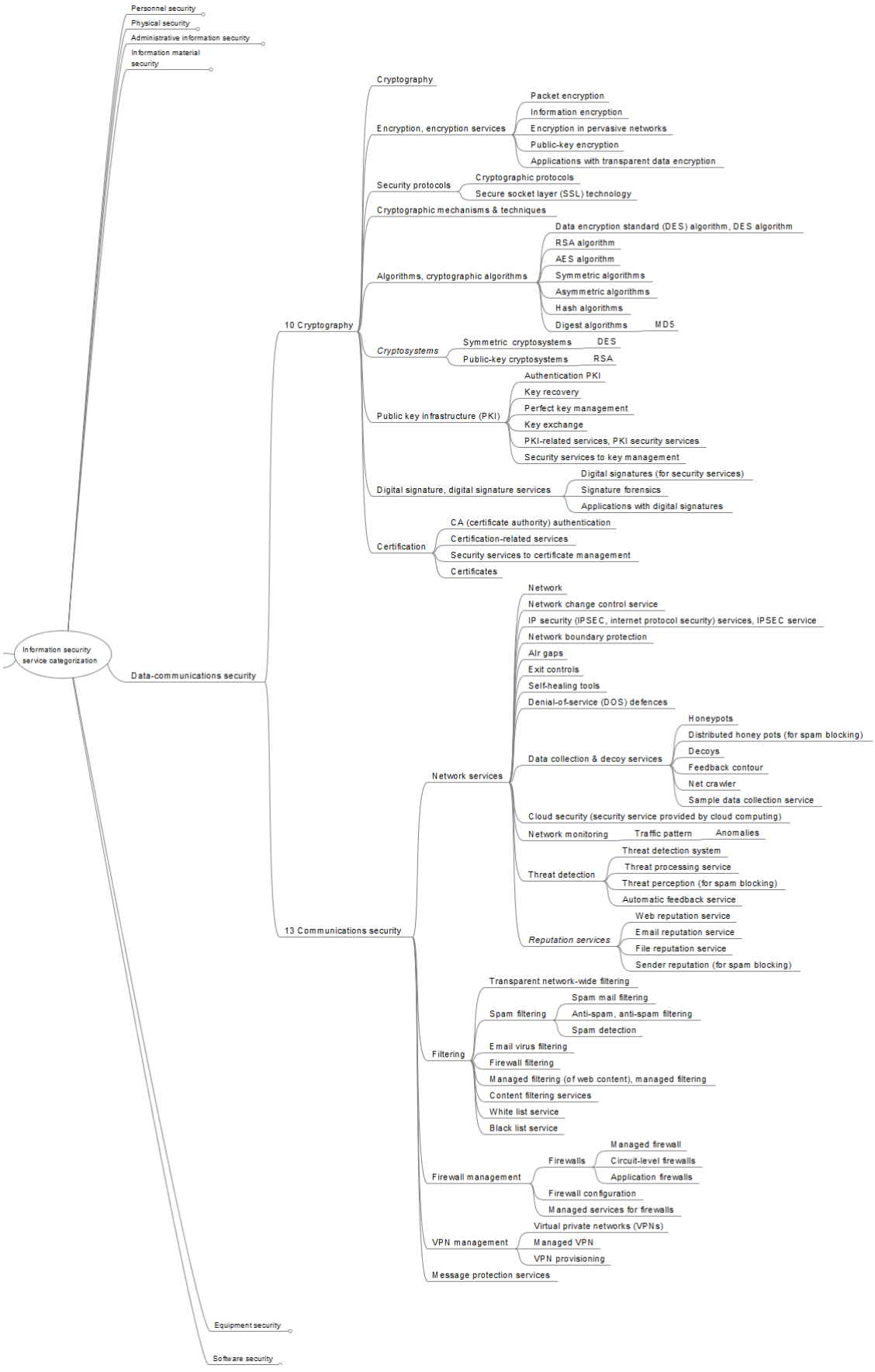
# APPENDIX 1.1 Main category: Operations security



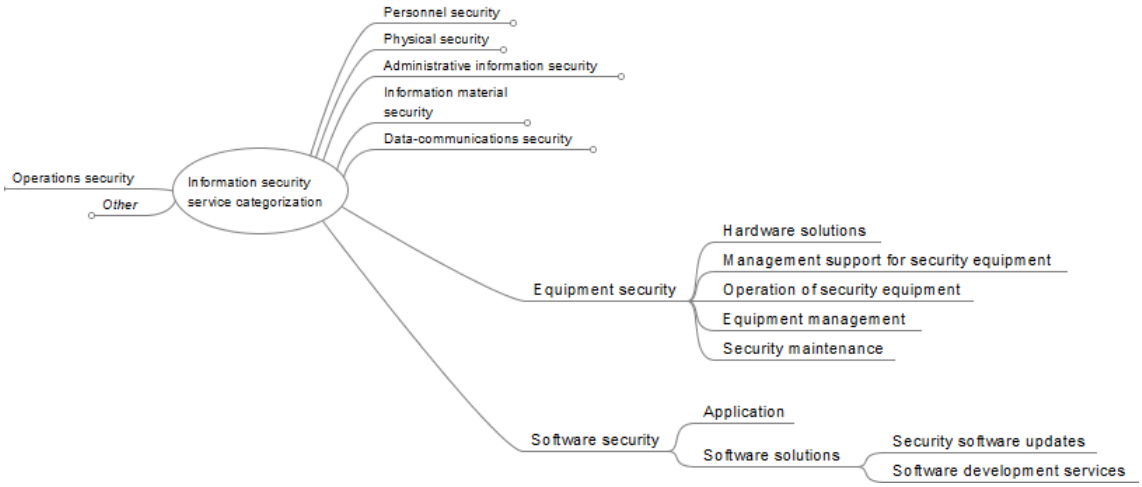
APPENDIX 1.2 Main categories: Personnel, Physical, Administrative information and Information material security



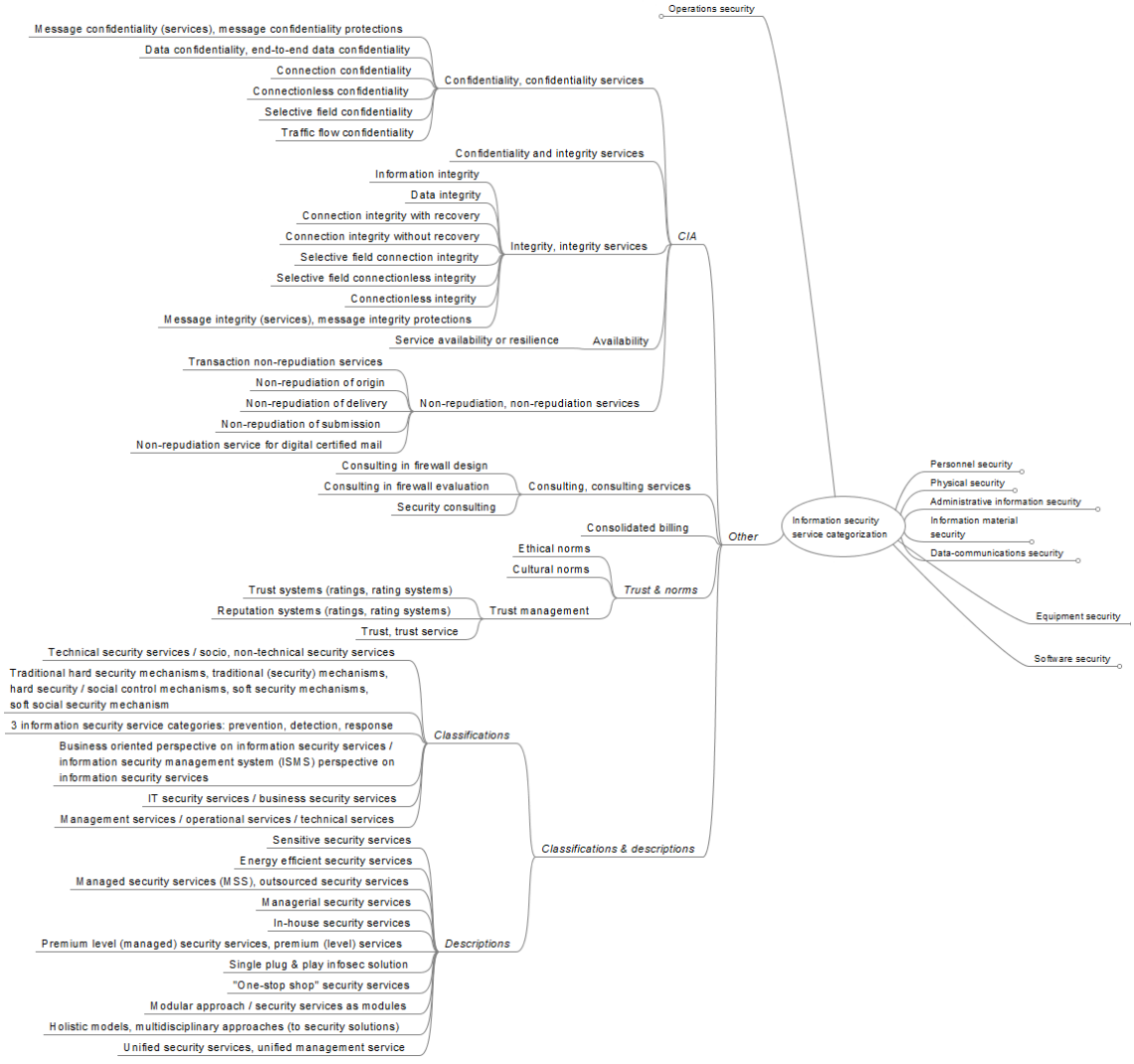
# APPENDIX 1.3 Main category: Data-communications security



APPENDIX 1.4 Main categories: Equipment and Software security




APPENDIX 1.5 Main category: Other



# APPENDIX 2.1 ISSeCa services by category

| Category | Information security service | Authors<br>Additional articles & articles referring to terms other than 'service' have been separated in the cell with extra space |
|---|---|---|
| Administrative information security / 18 Compliance | Certification (of the internal computer controls of an organization) | Chang & Lee (2003) |
| Administrative information security / 18 Compliance | Governance, risk and compliance | Buecker et al. (2007) |
| Administrative information security / 18 Compliance | Legal documents, contractual documents | Karokola et al. (2013) |
| Administrative information security / 18 Compliance | Legal frameworks, contractual frameworks | Karokola et al. (2011a) |
| Administrative information security / 18 Compliance | Operational guidelines, procedural guidelines | Karokola et al. (2011a), Karokola et al. (2013) |
| Administrative information security / 18 Compliance | Privacy protection | Jin et al. (2003) |
| Administrative information security / 18 Compliance / Privacy protection | Anonym (for privacy protection) | Jin et al. (2003) |
| Administrative information security / 18 Compliance / Privacy protection | Pseudonym (for privacy protection) | Jin et al. (2003) |
| Administrative information security / 18 Compliance / Privacy protection | Session privacy | Liping & Lei (2011) |
| Administrative information security / 5 Information security policies | Administrative policies, managerial policies | Karokola et al. (2011a), Karokola et al. (2013) |
| Administrative information security / 5 Information security policies | Business process and policy management | Buecker et al. (2007) |
| Administrative information security / 5 Information security policies | Security policy development, security policy application | Karyda et al. (2006) |
| Data-comms security / 10 Cryptography | Certification | Chang & Lee (2003) |
| Data-comms security / 10 Cryptography | Cryptographic algorithms | Tamilarasan et al. (2008) |
| Data-comms security / 10 Cryptography | Cryptographic mechanisms | Kovač & Trček (2009) (traditional security mechanisms) |
| Data-comms security / 10 Cryptography | Digital signature | Lin & Zhixin (2010) |
| Data-comms security / 10 Cryptography | Digital signature services | Liping & Lei (2011) |
| Data-comms security / 10 Cryptography | Encryption | Keeratiwintakorn & Krishnamurthy (2006)<br><br>Asgarnezhad et al. (2010) (cryptographic technique), Priescu et al. (2009) (layer of security) |
| Data-comms security / 10 Cryptography | Encryption service(s) | Karyda et al. (2006), Keeratiwintakorn & Krishnamurthy (2006), Liping & Lei (2011) |
| Data-comms security / 10 Cryptography | PKI | Liping & Lei (2011) |
| Data-comms security / 10 Cryptography | Public key infrastructure(s) | Liping & Lei (2011), Miguel et al. (2015) (solution) |
| Data-comms security / 10 Cryptography | Security protocols | Tamilarasan et al. (2008) |
| Data-comms security / 10 Cryptography | Algorithms | Xia & Hu (2006) |
| Data-comms security / 10 Cryptography | Cryptographic techniques | Asgarnezhad et al. (2010) |

| | | |
|---|---|---|
| Data-comms security / 10 Cryptography | Cryptography | Buecker et al. (2007) |
| Data-comms security / 10 Cryptography / Algorithms | AES algorithm | Tamilarasan et al. (2008) |
| Data-comms security / 10 Cryptography / Algorithms | Data encryption standard (DES) algorithm | Xia & Hu (2006) |
| Data-comms security / 10 Cryptography / Algorithms | DES algorithm | Tamilarasan et al. (2008) |
| Data-comms security / 10 Cryptography / Algorithms | Digest algorithms (e.g., MD5) | Deng et al. (1995) (mechanism to provide services) |
| Data-comms security / 10 Cryptography / Algorithms | RSA algorithm | Xia & Hu (2006), Tamilarasan et al. (2008) |
| Data-comms security / 10 Cryptography / Algorithms | Symmetric algorithm(s), asymmetric algorithm(s), hash algorithm(s) | Tamilarasan et al. (2008) (types of algorithms) |
| Data-comms security / 10 Cryptography / Certification | CA (certificate authority) authentication | Lin & Zhixin (2010) |
| Data-comms security / 10 Cryptography / Certification | Certificates | Liping & Lei (2011) |
| Data-comms security / 10 Cryptography / Certification | Certification-related services | Chang & Lee (2003) |
| Data-comms security / 10 Cryptography / Certification | Security services to certificate management | Liping & Lei (2011) |
| Data-comms security / 10 Cryptography / Cryptosystems | Symmetric cryptosystems (e.g., DES), public-key cryptosystems (e.g., RSA) | Deng et al. (1995) (mechanisms to provide services) |
| Data-comms security / 10 Cryptography / Digital signature | Applications with digital signatures | Liping & Lei (2011) |
| Data-comms security / 10 Cryptography / Digital signature | Digital signatures (for security services) | Peiris et al. (2008) |
| Data-comms security / 10 Cryptography / Digital signature | Signature forensics | Datta Ray et al. (2010) |
| Data-comms security / 10 Cryptography / Encryption | Applications with transparent data encryption | Liping & Lei (2011) |
| Data-comms security / 10 Cryptography / Encryption | Encryption in pervasive networks | Keeratiwintakorn & Krishnamurthy (2006) |
| Data-comms security / 10 Cryptography / Encryption | Information encryption | Lu et al. (2015) |
| Data-comms security / 10 Cryptography / Encryption | Packet encryption | Keeratiwintakorn & Krishnamurthy (2006) |
| Data-comms security / 10 Cryptography / Encryption | Public-key encryption | Chang & Lee (2003) |
| Data-comms security / 10 Cryptography / PKI | Authentication PKI | Lin & Zhixin (2010) |
| Data-comms security / 10 Cryptography / PKI | Key exchange | Lin & Zhixin (2010) |
| Data-comms security / 10 Cryptography / PKI | Key recovery | Liping & Lei (2011) |
| Data-comms security / 10 Cryptography / PKI | Perfect key management | Lin & Zhixin (2010) |
| Data-comms security / 10 Cryptography / PKI | PKI security services | Liping & Lei (2011) |
| Data-comms security / 10 Cryptography / PKI | PKI-related services | Chang & Lee (2003) |
| Data-comms security / 10 Cryptography / PKI | Security services to key management | Liping & Lei (2011) |
| Data-comms security / 10 Cryptography / Security protocols | Cryptographic protocols | Kovač & Trček (2009) (traditional security mechanisms) |
| Data-comms security / 10 Cryptography / Security protocols | Secure socket layer (SSL) technology | El Yamany & Capretz (2008) (traditional security technique) |
| Data-comms security / 13 Communications security | Filtering | Sidiroglou et al. (2007) |
| Data-comms security / 13 Communications security | Firewall management | Karyda et al. (2006), Oladapo et al. (2009) |
| Data-comms security / 13 Communications security | Network services | Vorakulpipat et al. (2014) |
| Data-comms security / 13 Communications security | VPN management | Karyda et al. (2006) |

| | | |
|---|---|---|
| Data-comms security / 13 Communications security | Message protection services | Buecker et al. (2007) |
| Data-comms security / 13 Communications security / Filtering | Black list service | Wang et al. (2010) |
| Data-comms security / 13 Communications security / Filtering | Content filtering services | Karyda et al. (2006) |
| Data-comms security / 13 Communications security / Filtering | Email virus filtering | Karyda et al. (2006) |
| Data-comms security / 13 Communications security / Filtering | Managed filtering (of web content), managed filtering | Choi & Seo (2005) |
| Data-comms security / 13 Communications security / Filtering | Spam filtering | Karyda et al. (2006) |
| Data-comms security / 13 Communications security / Filtering | Transparent network-wide filtering | Sidiroglou et al. (2007) |
| Data-comms security / 13 Communications security / Filtering | White list service | Wang et al. (2010) (technology/service) |
| Data-comms security / 13 Communications security / Filtering | Firewall filtering | Sidiroglou et al. (2007) |
| Data-comms security / 13 Communications security / Filtering / Spam filtering | Anti-spam, spam detection | Sidiroglou et al. (2007) |
| Data-comms security / 13 Communications security / Filtering / Spam filtering | Spam mail(s) filtering (based on cloud security), anti-spam filtering | Wang et al. (2010) |
| Data-comms security / 13 Communications security / Firewall mgt | Firewall configuration | Karyda et al. (2006) |
| Data-comms security / 13 Communications security / Firewall mgt | Firewalls | Karyda et al. (2006)<br><br>Priescu et al. (2009) (layer of security), Schultz (1995) (solutions, products), Wang et al. (2010) (traditional security technique) |
| Data-comms security / 13 Communications security / Firewall mgt | Managed services for firewalls | Karyda et al. (2006) |
| Data-comms security / 13 Communications security / Firewall mgt / Firewalls | Circuit-level firewalls, application firewalls | Schultz (1995) (solutions) |
| Data-comms security / 13 Communications security / Firewall mgt / Firewalls | Managed firewall | Choi & Seo (2005) |
| Data-comms security / 13 Communications security / Network services | Air gaps | Priescu et al. (2009) (solution) |
| Data-comms security / 13 Communications security / Network services | Cloud security (security service provided by cloud computing) | Wang et al. (2010) |
| Data-comms security / 13 Communications security / Network services | Data collection services: honeypot, net crawler, feedback contour | Wang et al. (2010) (technology/service) |
| Data-comms security / 13 Communications security / Network services | Decoy services: honeypots, decoys | Priescu et al. (2009) (solutions) |
| Data-comms security / 13 Communications security / Network services | Denial-of-service (DOS) defences | Priescu et al. (2009) (solution) |
| Data-comms security / 13 Communications security / Network services | Exit controls | Priescu et al. (2009) (solution) |
| Data-comms security / 13 Communications security / Network services | IP security (IPSEC, internet protocol security) services, IPSEC service | Chappell et al. (1999) |
| Data-comms security / 13 Communications security / Network services | Network boundary protection (incl. managed services for firewalls) | Karyda et al. (2006) |
| Data-comms security / 13 Communications security / Network services | Self-healing tools | Priescu et al. (2009) (solution) |

| | | |
|---|---|---|
| Data-comms security / 13 Communications security / Network services | Threat detection (based on cloud security) | Wang et al. (2010) |
| Data-comms security / 13 Communications security / Network services | Network monitoring | Karyda et al. (2006) |
| Data-comms security / 13 Communications security / Network services / Data collection & decoy services | Distributed honeypots (for spam blocking) | Wang et al. (2010) |
| Data-comms security / 13 Communications security / Network services / Data collection & decoy services | Sample data collection service | Wang et al. (2010) |
| Data-comms security / 13 Communications security / Network services / Network monitoring | Traffic pattern | Datta Ray et al. (2010) |
| Data-comms security / 13 Communications security / Network services / Network monitoring / Traffic pattern | Anomalies | Datta Ray et al. (2010) |
| Data-comms security / 13 Communications security / Network services / Reputation services | Sender reputation (for spam blocking) | Wang et al. (2010) |
| Data-comms security / 13 Communications security / Network services / Reputation services | Web reputation service, email reputation service, file reputation service | Wang et al. (2010) (technology/service) |
| Data-comms security / 13 Communications security / Network services / Threat detection | Automatic feedback service | Wang et al. (2010) (technology/service) |
| Data-comms security / 13 Communications security / Network services / Threat detection | Threat detection system (based on cloud security), threat processing service (based on cloud security) | Wang et al. (2010) |
| Data-comms security / 13 Communications security / Network services / Threat detection | Threat perception (for spam blocking) | Wang et al. (2010) |
| Data-comms security / 13 Communications security / VPN mgt | Managed VPN | Choi & Seo (2005) |
| Data-comms security / 13 Communications security / VPN mgt | Virtual private networks | El Yamany & Capretz (2008) (traditional security technique) |
| Data-comms security / 13 Communications security / VPN mgt | VPN provisioning | Sidiroglou et al. (2007) |
| Data-comms security / 13 Communications security / VPN mgt | VPN(s) | Karyda et al. (2006) (security installation), Wang et al. (2010) (traditional security technique) |
| Data-comms security / 13 Communications security/Network services | Network | Bahl & Wali (2013), Bahl & Wali (2014) |
| Data-comms security / 13 Communications security/Network services | Network change control service | Sun & Chen (2008) |
| Equipment security | Hardware solutions | Karokola et al. (2011a), Karokola et al. (2013) |
| Equipment security | Management support for security equipment, operation of security equipment, equipment management | Choi & Seo (2005) |
| Equipment security | Security maintenance | Choi & Seo (2005) |
| Information material security / 8 Asset management | Data archiving, data restoration | Karyda et al. (2006) |
| Information material security / 8 Asset management | Data classification | Karyda et al. (2006) |
| Information material security / 8 Asset management | Data protection and disclosure control | Buecker et al. (2007) |
| Information material security / 8 Asset management | Distributed power mass data storage | Wang et al. (2010) |
| Information material security / 8 Asset management | Media protection | Oladapo et al. (2009) |

| | | |
|---|---|---|
| Information material security / 8 Asset management | Time stamping | Miguel et al. (2015) |
| Information material security / 8 Asset management / Data protection & disclosure control | Data protection services | Buecker et al. (2007) |
| Information material security / 8 Asset management / Data protection & disclosure control / Data protection services | Data isolation support | Buecker et al. (2007) |
| Information material security / 8 Asset management / Time stamping | Timestamps | Deng et al. (1995) (mechanism to provide services) |
| Operations security / 12 Operations security / Monitoring | Remote & local security control for infrastructure: databases, networks, servers | Choi & Seo (2005) |
| Operations security / 12 Operations / Monitoring | Privileged ID monitoring service, ID activity monitoring service | Sun & Chen (2008) |
| Operations security / 12 Operations security | Audit | Claassen et al. (1992), Jin et al. (2003), Oladapo et al. (2009) |
| Operations security / 12 Operations security | Audit service(s) | Asgarnezhad et al. (2010), El Yamany & Capretz (2008), Miguel et al. (2015)<br><br>Buecker et al. (2007) |
| Operations security / 12 Operations security | Configuration management | Oladapo et al. (2009) |
| Operations security / 12 Operations security | Helpdesk services | Vorakulpipat et al. (2014) |
| Operations security / 12 Operations security | Managed scanning (analysis of vulnerability), managed scanning | Choi & Seo (2005) |
| Operations security / 12 Operations security | Management of security systems | Karyda et al. (2006) |
| Operations security / 12 Operations security | Monitoring | Datta Ray et al. (2010) |
| Operations security / 12 Operations security | Monitoring service(s) | Moulton & Coles (2003) |
| Operations security / 12 Operations security | Server management | Karyda et al. (2006) |
| Operations security / 12 Operations security / Audit | External connection review service | Sun & Chen (2008) |
| Operations security / 12 Operations security / Audit | IT auditing | Karyda et al. (2006) |
| Operations security / 12 Operations security / Audit | Security audit | Claassen et al. (1992), Deng et al. (1995) |
| Operations security / 12 Operations security / Managed scanning | Automated vulnerability detection, automated vulnerability mitigation | Sidiroglou et al. (2007) |
| Operations security / 12 Operations security / Management of security systems | Secure systems and networks | Buecker et al. (2007) |
| Operations security / 12 Operations security / Monitoring | Intruder detection | Chang & Lee (2003) |
| Operations security / 12 Operations security / Monitoring | Intrusion detection systems management | Karyda et al. (2006) |
| Operations security / 12 Operations security / Monitoring | IPS (intrusion prevention system) | Wang et al. (2010) (traditional security technique) |
| Operations security / 12 Operations security / Monitoring | Monitoring for service uptime & availability (to detect DOS attacks & service disruption) | Moulton & Coles (2003) |
| Operations security / 12 Operations security / Monitoring | Monitoring of security systems | Karyda et al. (2006) |
| Operations security / 12 Operations security / Monitoring / Behaviour analysis | Large-scale behaviour analysis (of users, traffic etc.) | Sidiroglou et al. (2007) |
| Operations security / 12 Operations security / Monitoring / Behaviour analysis | Relative analysis of behaviour service | Wang et al. (2010) (technology/service) |

| | | |
|---|---|---|
| Operations security / 12 Operations security / Monitoring / Intrusion detection systems mgt | Distributed intrusion detection systems | Sidiroglou et al. (2007) |
| Operations security / 12 Operations security / Monitoring / Intrusion detection systems mgt | IDS (intrusion detection system) | Wang et al. (2010) (traditional security technique) |
| Operations security / 12 Operations security / Monitoring / Intrusion detection systems mgt | Intrusion detection | Deng et al. (1995), Lu et al. (2015), Moulton & Coles (2003), Oladapo et al. (2009) |
| Operations security / 12 Operations security / Monitoring / Intrusion detection systems mgt | Intrusion monitoring | Karyda et al. (2006) |
| Operations security / 12 Operations security / Monitoring / Intrusion detection systems mgt | Managed IDS (intrusion detection system) | Choi & Seo (2005) |
| Operations security / 12 Operations security / Monitoring / Intrusion detection systems mgt / Intrusion detection | Host-based intrusion detection software | Moulton & Coles (2003) |
| Operations security / 12 Operations security / Monitoring / Intrusion detection systems mgt / Intrusion detection | Intrusion detection software | Moulton & Coles (2003) |
| Operations security / 12 Operations security / Monitoring / Intrusion detection systems mgt / Intrusion detection | Network intrusion detection software | Moulton & Coles (2003) |
| Operations security / 12 Operations security / Security analysis | Audit logging service | Buecker et al. (2007) |
| Operations security / 12 Operations security / Security analysis | Intelligent mining service of security log | Wang et al. (2010) |
| Operations security / 12 Operations security / Security analysis | Intelligent security analysis service, intelligent analysis service of security log | Wang et al. (2010) |
| Operations security / 12 Operations security / Security analysis | Security estimation, security estimation services | Chang & Lee (2003) |
| Operations security / 12 Operations security / Security analysis | Decision analysis | Datta Ray et al. (2010) |
| Operations security / 12 Operations security / Server mgt | Server change control service | Sun & Chen (2008) |
| Operations security / 12 Operations security / Server mgt | Server configuration | Moulton & Coles (2003) |
| Operations security / 12 Operations security / Server mgt / Server configuration | Server configuration software | Moulton & Coles (2003) |
| Operations security / 12 Operations security / Virus & worm protection | Antivirus mechanism | Karokola et al. (2011a) |
| Operations security / 12 Operations security / Virus & worm protection | Antivirus system (based on cloud security) | Wang et al. (2010) |
| Operations security / 12 Operations security / Virus & worm protection | Anti-virus, virus detection | Sidiroglou et al. (2007) |
| Operations security / 12 Operations security / Virus & worm protection | Managed antivirus | Choi & Seo (2005) |
| Operations security / 12 Operations security / Virus & worm protection | Virus protection | Karyda et al. (2006) |
| Operations security / 12 Operations security / Virus & worm protection | Worm vaccine, worm detection, email worm detection | Sidiroglou et al. (2007) |
| Operations security / 14 System acquisition, development & maintenance | Application integration services | Chang & Lee (2003) |
| Operations security / 14 System acquisition, development & maintenance | Application isolation support | Buecker et al. (2007) |
| Operations security / 14 System acquisition, development & maintenance | Penetration testing | Karyda et al. (2006) |

| | | |
|---|---|---|
| Operations security / 14 System acquisition, development & maintenance | Security upgrades | Karyda et al. (2006) |
| Operations security / 14 System acquisition, development & maintenance | System integration services (for integrating applications or networks), system integration | Chang & Lee (2003) |
| Operations security / 16 Information security incident mgt | Analysis of security attack events, analysis of security attack incidents | Choi & Seo (2005) |
| Operations security / 16 Information security incident mgt | Emergency response | Karyda et al. (2006) |
| Operations security / 16 Information security incident mgt | Incident management (incl. emergency response) | Karyda et al. (2006) |
| Operations security / 16 Information security incident mgt / Analysis of security attack events & incidents | Attack inference | Sidiroglou et al. (2007) |
| Operations security / 17 Information security aspects of business continuity mgt | Backup for service continuity & restoration | Datta Ray et al. (2010) |
| Operations security / 17 Information security aspects of business continuity mgt | Business continuity planning | Karyda et al. (2006) |
| Operations security / 17 Information security aspects of business continuity mgt | Contingency planning | Karyda et al. (2006) |
| Operations security / 17 Information security aspects of business continuity mgt | Disaster recovery | Karyda et al. (2006) |
| Operations security / 17 Information security aspects of business continuity mgt | Failure control | Miguel et al. (2015) |
| Operations security / 17 Information security aspects of business continuity mgt | Redundancies for service continuity & restoration | Datta Ray et al. (2010) |
| Operations security / 9 Access control | Access control | Claassen et al. (1992), Datta Ray et al. (2010), Deng et al. (1995), Jin et al. (2003), Liping & Lei (2011), Lu et al. (2015), Miguel et al. (2015), Oladapo et al. (2009), Peiris et al. (2008)<br><br>Jeong et al. (2010) (method), Kovač & Trček (2009) (traditional security mechanism), Shaikh et al. (2005) |
| Operations security / 9 Access control | Access control service | Deng et al. (1995) |
| Operations security / 9 Access control | Authorization | AbdElnapi et al. (2016), Asgarnezhad et al. (2010), Datta Ray et al. (2010), Jin et al. (2003)<br><br>Kovač & Trček (2009) (security techniques), Shaikh et al. (2005) |
| Operations security / 9 Access control | Authorization service(s) | Asgarnezhad et al. (2010), El Yamany & Capretz (2008)<br><br>Buecker et al. (2007) |
| Operations security / 9 Access control | Identification | Miguel et al. (2015) |
| Operations security / 9 Access control | Identity and access | Buecker et al. (2007) |
| Operations security / 9 Access control | Passwords | Liping & Lei (2011) |
| Operations security / 9 Access control | Unified authentication and identity management | Jin et al. (2003) |
| Operations security / 9 Access control | User provisioning | Shaikh et al. (2005) |

| | | |
|---|---|---|
| Operations security / 9 Access control | Authentication | Asgarnezhad et al. (2010), Chappell et al. (1999), Claassen et al. (1992), Datta Ray et al. (2010), Deng et al. (1995), Jin et al. (2003), Liping & Lei (2011), Miguel et al. (2015), Peiris et al. (2008), Rachedi & Benslimane (2016), Tamilarasan et al. (2008)<br><br>Kovač & Trček (2009) (traditional security mechanism), Shaikh et al. (2005) |
| Operations security / 9 Access control | Authentication service(s) | Asgarnezhad et al. (2010), Deng et al. (1995), El Yamany & Capretz (2008), Jin et al. (2003)<br><br>Buecker et al. (2007) |
| Operations security / 9 Access control / Access control | Access control mechanism | Karokola et al. (2011a) |
| Operations security / 9 Access control / Access control | Access control techniques | Kovač & Trček (2009) |
| Operations security / 9 Access control / Access control | Access controls: Mandatory access control, discretionary access control | Deng et al. (1995) |
| Operations security / 9 Access control / Access control | Directory management service | Sun & Chen (2008) |
| Operations security / 9 Access control / Access control | Network access control service | Sun & Chen (2008) |
| Operations security / 9 Access control / Access control | Object access control | Deng et al. (1995) |
| Operations security / 9 Access control / Access control | Privilege management | Jin et al. (2003) |
| Operations security / 9 Access control / Access control | Single sign on | Shaikh et al. (2005) |
| Operations security / 9 Access control / Access control | Single-sign-on (SSO) | Jin et al. (2003) |
| Operations security / 9 Access control / Access control | User access management | Karyda et al. (2006) |
| Operations security / 9 Access control / Authentication | Authentication techniques | Kovač & Trček (2009) |
| Operations security / 9 Access control / Authentication | Client authentication | Deng et al. (1995) |
| Operations security / 9 Access control / Authentication | Data origin authentication | Claassen et al. (1992) |
| Operations security / 9 Access control / Authentication | End-to-end authentication and integrity service | Rachedi & Benslimane (2016) |
| Operations security / 9 Access control / Authentication | Host authentication | Claassen et al. (1992) |
| Operations security / 9 Access control / Authentication | Identity authentication | Lu et al. (2015) |
| Operations security / 9 Access control / Authentication | Message authentication | Keeratiwintakorn & Krishnamurthy (2006) |
| Operations security / 9 Access control / Authentication | Message authentication service(s) | Deng et al. (1995), Keeratiwintakorn & Krishnamurthy (2006) |
| Operations security / 9 Access control / Authentication | Message origin authentication | Deng et al. (1995) |
| Operations security / 9 Access control / Authentication | Mutual authentication | Rachedi & Benslimane (2016) |
| Operations security / 9 Access control / Authentication | Object authentication | Deng et al. (1995) |
| Operations security / 9 Access control / Authentication | Peer entity authentication | Claassen et al. (1992) |
| Operations security / 9 Access control / Authentication | Process authentication | Claassen et al. (1992) |
| Operations security / 9 Access control / Authentication | Relayed-nodes authentication and integrity service | Rachedi & Benslimane (2016) |

| | | |
|---|---|---|
| Operations security / 9 Access control / Authentication | User authentication | Claassen et al. (1992) |
| Operations security / 9 Access control / Authorization | Authorization and privacy services | Buecker et al. (2007) |
| Operations security / 9 Access control / Authorization | Authorization techniques | Kovač & Trček (2009) (security techniques) |
| Operations security / 9 Access control / Identification | Biometric identification | Jin et al. (2003) (authentication mechanism) |
| Operations security / 9 Access control / Identification | ID management, identity management | Jin et al. (2003) |
| Operations security / 9 Access control / Identification | Identity management services | Jin et al. (2003) |
| Operations security / 9 Access control / Identification | Identity service(s) | Asgarnezhad et al. (2010)<br><br>Buecker et al. (2007) |
| Operations security / 9 Access control / Identification / Biometric identification | Biometric models | Miguel et al. (2015) (solution) |
| Operations security / 9 Access control / Unified authentication & identity mgt | Unified authentication and identity management service(s), authentication and identity management service | Jin et al. (2003) |
| Other | Consolidated billing | Jin et al. (2003) |
| Other | Consulting | Chang & Lee (2003) |
| Other | Consulting services | Vorakulpipat et al. (2014) |
| Other / CIA | Availability | AbdElnapi et al. (2016), Datta Ray et al. (2010), Lee et al. (2006), Miguel et al. (2015), Wahab et al. (2013) |
| Other / CIA | Confidentiality | AbdElnapi et al. (2016), Asgarnezhad et al. (2010), Chappell et al. (1999), Claassen et al. (1992), Keeratiwintakorn & Krishnamurthy (2006), Lee et al. (2006), Miguel et al. (2015), Peiris et al. (2008), Rachedi & Benslimane (2016), Tamilarasan et al. (2008), Datta Ray et al. (2010)<br><br>Shaikh et al. (2005), Buecker et al. (2007) |
| Other / CIA | Confidentiality and integrity services | Buecker et al. (2007) |
| Other / CIA | Confidentiality service(s) | Asgarnezhad et al. (2010), Rachedi & Benslimane (2016)<br><br>Buecker et al. (2007) |
| Other / CIA | Integrity | AbdElnapi et al. (2016), Claassen et al. (1992), Lee et al. (2006), Liping & Lei (2011), Miguel et al. (2015), Peiris et al. (2008), Rachedi & Benslimane (2016), Tamilarasan et al. (2008)<br><br>Shaikh et al. (2005), Buecker et al. (2007) |
| Other / CIA | Integrity services | Asgarnezhad et al. (2010)<br><br>Buecker et al. (2007) |
| Other / CIA | Non-repudiation | AbdElnapi et al. (2016), Claassen et al. (1992), Lin & Zhixin (2010), Miguel et al. (2015), Peiris et al. (2008), Tamilarasan et al. (2008)<br><br>Shaikh et al. (2005) |
| Other / CIA | Non-repudiation service(s) | Buecker et al. (2007) |
| Other / CIA / Availability | Service availability (resilience) | Sidiroglou et al. (2007) |
| Other / CIA / Confidentiality | Connection confidentiality | Claassen et al. (1992) |

| | | |
|---|---|---|
| Other / CIA / Confidentiality | Connectionless confidentiality | Claassen et al. (1992) |
| Other / CIA / Confidentiality | Data confidentiality | Wahab et al. (2013) |
| Other / CIA / Confidentiality | End-to-end data confidentiality | Rachedi & Benslimane (2016) |
| Other / CIA / Confidentiality | Message confidentiality | Liping & Lei (2011), Deng et al. (1995) |
| Other / CIA / Confidentiality | Message confidentiality protections | Deng et al. (1995) |
| Other / CIA / Confidentiality | Message confidentiality services | Deng et al. (1995) |
| Other / CIA / Confidentiality | Selective field confidentiality | Claassen et al. (1992) |
| Other / CIA / Confidentiality | Traffic flow confidentiality | Claassen et al. (1992) |
| Other / CIA / Integrity | Connection integrity with recovery | Claassen et al. (1992) |
| Other / CIA / Integrity | Connection integrity without recovery | Claassen et al. (1992) |
| Other / CIA / Integrity | Connectionless integrity | Claassen et al. (1992) |
| Other / CIA / Integrity | Data integrity | AbdElnapi et al. (2016), Rachedi & Benslimane (2016), Wahab et al. (2013) |
| Other / CIA / Integrity | Information integrity | Liping & Lei (2011) |
| Other / CIA / Integrity | Message integrity | Deng et al. (1995) |
| Other / CIA / Integrity | Message integrity protections | Deng et al. (1995) |
| Other / CIA / Integrity | Message integrity services | Deng et al. (1995) |
| Other / CIA / Integrity | Selective field connection integrity | Claassen et al. (1992) |
| Other / CIA / Integrity | Selective field connectionless integrity | Claassen et al. (1992) |
| Other / CIA / Non-repudiation | Non-repudiation (delivery), non-repudiation of delivery | Claassen et al. (1992), Peiris et al. (2008) |
| Other / CIA / Non-repudiation | Non-repudiation (origin), non-repudiation of origin | Claassen et al. (1992), Peiris et al. (2008) |
| Other / CIA / Non-repudiation | Non-repudiation of submission | Peiris et al. (2008) |
| Other / CIA / Non-repudiation | Non-repudiation service for digital certified mail | Buecker et al. (2007) |
| Other / CIA / Non-repudiation | Transaction non-repudiation services | Liping & Lei (2011) |
| Other / Classifications & descriptions / Classifications | 3 Information security service categories: prevention, detection, response | Datta Ray et al. (2010) |
| Other / Classifications & descriptions / Classifications | Business oriented perspective on information security services | Voralkupipat et al. |
| Other / Classifications & descriptions / Classifications | Business security services | Buecker et al. (2007) (information security component) |
| Other / Classifications & descriptions / Classifications | Information security management system (ISMS) perspective on information security services | Voralkupipat et al. |
| Other / Classifications & descriptions / Classifications | IT security services | Buecker et al. (2007) (information security component) |
| Other / Classifications & descriptions / Classifications | Management services | Bowen et al. (2006) (information security service category) |
| Other / Classifications & descriptions / Classifications | Operational services | Bowen et al. (2006) (information security service category) |
| Other / Classifications & descriptions / Classifications | Socio / non-technical security services | Karokola et al. (2011a), Karokola et al. (2013) (security services or aspects) |
| Other / Classifications & descriptions / Classifications | Soft social security mechanism, soft security mechanisms, social control mechanisms | Kovač & Trček (2009) |
| Other / Classifications & descriptions / Classifications | Technical security services | Karokola et al. (2011a), Karokola et al. (2013) (security services or aspects) |
| Other / Classifications & descriptions / Classifications | Technical services | Bowen et al. (2006) (information security service category) |
| Other / Classifications & descriptions / Classifications | Traditional hard security mechanisms, traditional (security) mechanisms, hard security | Kovač & Trček (2009) |
| Other / Classifications & descriptions / Descriptions | "One-stop shop" security services | Sidiroglou et al. (2007) |
| Other / Classifications & descriptions / Descriptions | Energy efficient security service(s) | Keeratiwintakorn & Krishnamurthy (2006) |

| | | |
|---|---|---|
| Other / Classifications & descriptions / Descriptions | Holistic models, multidisciplinary approaches (to security solutions) | Miguel et al. (2015) (solution) |
| Other / Classifications & descriptions / Descriptions | In-house security services | Karyda et al. (2006) |
| Other / Classifications & descriptions / Descriptions | Managed security service(s) (MSS) | Choi & Seo (2005), Karyda et al. (2006) |
| Other / Classifications & descriptions / Descriptions | Managerial security services | Choi & Seo (2005) |
| Other / Classifications & descriptions / Descriptions | Modular approach (security services as modules) | Sidiroglou et al. (2007) |
| Other / Classifications & descriptions / Descriptions | Outsourced security services | Karyda et al. (2006) |
| Other / Classifications & descriptions / Descriptions | Premium level (of) managed security services, premium level security services, premium (level) services | Moulton & Coles (2003) |
| Other / Classifications & descriptions / Descriptions | Sensitive security services | Oladapo et al. (2009) |
| Other / Classifications & descriptions / Descriptions | Single plug & play information security solution | Schultz (1995) |
| Other / Classifications & descriptions / Descriptions | Unified security services, unified management service | Jin et al. (2003) |
| Other / Consulting | Consulting in firewall design, consulting in firewall evaluation | Schultz (1995) |
| Other / Consulting | Security consulting | Choi & Seo (2005) |
| Other / Trust & norms | Ethical norms, cultural norms | Karokola et al. (2011a), Karokola et al. (2013) |
| Other / Trust & norms | Trust management | Buecker et al. (2007) |
| Other / Trust & norms / Trust mgt | Reputation systems (ratings, rating systems) | Kovač & Trček (2009) (social control mechanism) |
| Other / Trust & norms / Trust mgt | Trust service | Buecker et al. (2007) |
| Other / Trust & norms / Trust mgt | Trust, trust systems (ratings, rating systems) | Kovač & Trček (2009) (social control mechanisms) |
| Personnel security / 7 Human resource security | People (as required contractually) | Bahl & Wali (2013), Bahl & Wali (2014) |
| Personnel security / 7 Human resource security | Security awareness | Oladapo et al. (2009) |
| Personnel security / 7 Human resource security / Security awareness | Awareness programmes | Karokola et al. (2011a), Karokola et al. (2013) |
| Personnel security / 7 Human resource security / Security awareness | Security education | Karyda et al. (2006) |
| Personnel security / 7 Human resource security / Security awareness | Security training | Karyda et al. (2006), Oladapo et al. (2009) |
| Physical security / 11 Physical & environmental security | Physical | Bahl & Wali (2013), Bahl & Wali (2014) |
| Physical security / 11 Physical & environmental security | Physical security | Oladapo et al. (2009) |
| Software security | Application | Bahl & Wali (2013), Bahl & Wali (2014) |
| Software security | Software solutions | Karokola et al. (2011a), Karokola et al. (2013) |
| Software security / Software solutions | Security software updates | Moulton & Coles (2003) |
| Software security / Software solutions | Software development services | Vorakulpipat et al. (2014) |

# APPENDIX 2.2 ISSeCa services by author

| Authors | Services |
|---|---|
| AbdElnapi et al. (2016) | Authorization, availability, confidentiality, data integrity, integrity, non-repudiation |
| Asgarnezhad et al. (2010) | Audit services, authentication, authentication services, authorization, authorization service(s), confidentiality, confidentiality service(s), cryptographic techniques, encryption (cryptographic technique), identity services, integrity services |
| Bahl & Wali (2013) | Application, network, people (as required contractually), physical |
| Bahl & Wali (2014) | Application, network, people (as required contractually), physical |
| Bowen et al. (2006) | **Classifications:** Management services, operational services, technical services |
| Buecker et al. (2007) | **Classifications:** Business security services (information security components), IT security services (information security components)<br><br>**IT security services:**<br>Application isolation support, audit service(s), audit logging service, authentication service(s), authorization and privacy services, authorization services, confidentiality services, confidentiality, confidentiality and integrity services, cryptography, data isolation support, data protection services, identity service(s), integrity, integrity services, message protection services, non-repudiation service(s), non-repudiation service for digital certified mail<br><br>**Business security services:**<br>Business process and policy management; data protection and disclosure control; governance, risk and compliance; identity and access; secure systems and networks; trust management; trust service |
| Chang & Lee (2003) | Application integration services, certification, certification (of the internal computer controls of an organization), certification related services, consulting, intruder detection, PKI-related services, public-key encryption, security estimation, security estimation services, system integration, system integration services (for integrating applications or networks) |
| Chappell et al. (1999) | Authentication, confidentiality, IP security (IPSEC) services, IPSEC service |
| Choi & Seo (2005) | **Descriptions:** Managed security service(s) (MSS), managerial security services<br><br>**Managed security services (MSS):**<br>Analysis of security attack events, managed antivirus, managed filtering, managed filtering (of web content), managed firewall, managed IDS (intrusion detection system), managed scanning, managed scanning (analysis of vulnerability), managed VPN, management support for security equipment, operation of security equipment, security maintenance<br><br>Remote and local security control for infrastructure such as networks, servers and databases<br><br>**Managerial security services:**<br>Analysis of security attack incidents, equipment management, security consulting |
| Claassen et al. (1992) | Access control, audit, security audit<br><br>Authentication, user authentication, process authentication, host authentication, peer entity authentication, data origin authentication<br><br>Confidentiality, connection confidentiality, connectionless confidentiality, selective field confidentiality, traffic flow confidentiality<br><br>Non-repudiation, non-repudiation (origin), non-repudiation (delivery)<br><br>Integrity, connection integrity with recovery, connection integrity without recovery, selective field connection integrity, connectionless integrity, selective field connectionless integrity |
| Datta Ray et al. (2010) | **Classifications:** Detection, prevention, response<br><br>Anomalies, access control, authentication, authorization, availability, backup for service continuity & restoration, confidentiality, decision analysis, monitoring, traffic pattern, redundancies for service continuity & restoration, signature forensics |
| Deng et al. (1995) | Access control, access control service, object access control<br>Access controls: Mandatory access control, discretionary access control |

| | |
|---|---|
| | Authentication, authentication service, client authentication, message authentication services, message origin authentication, object authentication<br><br>Message confidentiality, message confidentiality protections, message confidentiality services<br><br>Message integrity, message integrity protections, message integrity services<br><br>Intrusion detection, security audit<br><br>Digest algorithms (e.g., MD5) (mechanism to provide services)<br>Public-key cryptosystems (e.g., RSA) (mechanism to provide services)<br>Symmetric cryptosystems (e.g., DES) (mechanism to provide services)<br>Timestamps (mechanism to provide services) |
| El Yamany & Capretz (2008) | Audit service, authentication service, authorization service<br><br>Secure sockets layer (SSL) technology (traditional security technique), virtual private networks (traditional security technique) |
| Jeong et al. (2010) | Access control (method) |
| Jin et al. (2003) | **Descriptions:** Unified management service, unified security services<br><br>Access control, audit, anonym (for privacy protection), authentication, authentication service(s), authorization, biometric identification (authentication mechanism), consolidated billing, ID management, identity management, identity management services, privacy protection, privilege management, pseudonym (for privacy protection), single-sign-on (SSO), unified authentication and identity management, unified authentication and identity management service(s), authentication and identity management service |
| Karokola et al. (2011a) | **Classifications:** Socio / non-technical security services (or aspects), technical security services (or aspects)<br><br>**Socio/non-technical:** Administrative policies, awareness programmes, contractual frameworks, cultural norms, ethical norms, legal frameworks, managerial policies, operational guidelines, procedural guidelines<br><br>**Technical:** Access control mechanism, antivirus mechanism, hardware solutions, software solutions |
| Karokola et al. (2013) | **Classifications:** Socio / non-technical security services (or aspects), technical security services (or aspects)<br><br>**Socio / non-technical:** Administrative policies, awareness programmes, contractual documents, cultural norms, ethical norms, legal documents, managerial policies, operational guidelines, procedural guidelines<br><br>**Technical:** Hardware solutions, software solutions |
| Karyda et al. (2006) | **Descriptions:** In-house services, managed security services (MSS), outsourced services<br><br>Business continuity planning, content filtering services, contingency planning, data archiving, data classification, data restoration, disaster recovery, email virus filtering, emergency response, encryption services, firewalls, firewall configuration, firewall management, incident management (incl. emergency response), intrusion detection systems management, intrusion monitoring, IT auditing, managed services for firewalls, management of security systems, monitoring of security systems, network boundary protection (incl. managed services for firewalls), network monitoring, penetration testing, security education, security policy application, security policy development, security training, security upgrades, server management, spam filtering, user access management, virus protection, VPN management, VPNs (security installation) |
| Keeratiwintakorn & Krishnamurthy (2006) | **Descriptions:** Energy efficient security service(s)<br><br>Encryption, encryption in pervasive networks, encryption service, confidentiality, message authentication, message authentication service, packet encryption |
| Kovač & Trček (2009) | **Classifications:** Hard security, social control mechanisms, soft security mechanisms, soft social security mechanism, traditional hard security mechanisms, traditional (security) mechanisms<br><br>**Hard security:**<br>Access control (traditional security mechanism), access control techniques, authentication (traditional security mechanism), authentication techniques, authorization, authori- |

| | |
|---|---|
| | zation techniques, cryptographic protocols (traditional security mechanism), cryptographic mechanisms (traditional security mechanism)<br><br>**Soft security:**<br>Reputation systems (social control mechanism), trust (soft social security mechanism), trust systems (social control mechanism) |
| Lee et al. (2006) | Availability, confidentiality, integrity |
| Lin & Zhixin (2010) | Authentication PKI, CA (certificate authority) authentication, digital signature, key exchange, non-repudiation, perfect key management |
| Liping & Lei (2011) | Access control, applications with digital signatures, applications with transparent data encryption, authentication, certificates, digital signature services, encryption services, information integrity, integrity, key recovery, message confidentiality, passwords, PKI, public key infrastructure, PKI security services, security services to certificate management, security services to key management, session privacy, transaction non-repudiation services |
| Lu et al. (2015) | Access control, identity authentication, information encryption, intrusion detection |
| Miguel et al. (2015) | **Descriptions:** Holistic models, multidisciplinary approaches to security solutions (solution)<br><br>Access control, audit service, authentication, availability, biometric models (solution), confidentiality, failure control, integrity, non-repudiation, identification, public key infrastructures (solution), time stamping |
| Moulton & Coles (2003) | **Classifications:** Premium level (of) managed security services, premium level security services, premium (level) services<br><br>Host-based intrusion detection software, intrusion detection, intrusion detection software, monitoring for server uptime & availability (to detect DOS attacks & service disruption),<br>monitoring service(s), network intrusion detection software, security software updates, server configuration, server configuration software |
| Oladapo et al. (2009) | **Descriptions:** Sensitive security services<br><br>Access control, audit, configuration management, firewall management, intrusion detection, media protection, physical security, security awareness, security training |
| Peiris et al. (2008) | Access control, authentication, confidentiality, digital signatures (for security services), integrity, non-repudiation, non-repudiation of delivery, non-repudiation of origin, non-repudiation of submission |
| Priescu et al. (2009) | Air gaps (solution), denial-of-service defences (DOS) (solution), encryption (layer of security), exit controls (solution), firewalls (layer of security), self-healing tools (solution)<br><br>Decoy services: Decoys, honeypots (solutions) |
| Rachedi & Benslimane (2016) | Authentication, confidentiality, confidentiality service, end-to-end authentication and integrity service, end-to-end data confidentiality, data integrity, integrity, mutual authentication, relayed nodes authentication and integrity service |
| Schultz (1995) | **Description**: Single plug & play information security solution<br><br>Application firewalls (solutions), circuit level firewalls (solutions), consulting in firewall design, consulting in firewall evaluation, firewalls (solutions, products) |
| Shaikh et al. (2005) | Access control (authorization), authentication, confidentiality, integrity, non-repudiation, single sign on, user provisioning |
| Sidiroglou et al. (2007) | **Descriptions:** Modular approach (security services as modules), one-stop shop for security services<br><br>Anti-spam, anti-virus, attack inference, automated vulnerability detection, automated vulnerability mitigation, distributed intrusion detection systems, email worm detection, filtering, firewall filtering, large-scale behaviour analysis (of users, traffic etc.), service availability (resilience), spam detection, transparent network-wide filtering, virus detection, VPN provisioning, worm detection, worm vaccine |
| Sun & Chen (2008) | Directory management service, external connection review service, ID activity monitoring service, network access control service, network change control service, privileged ID monitoring service, server change control service |
| Tamilarasan et al. (2008) | Authentication, confidentiality, integrity, non-repudiation, security protocols<br><br>AES algorithm, cryptographic algorithms, DES algorithm, RSA algorithm<br>Asymmetric algorithm(s), hash algorithm(s), symmetric algorithm(s) (types of algorithms) |

| | |
|---|---|
| Wahab et al. (2013) | Availability, data confidentiality, data integrity |
| Wang et al. (2010) | Anti-spam filtering, automatic feedback service (technology/service), anti-virus system (based on cloud security), black list service, cloud security, data collection service (honeypot, net crawler, feedback contour) (technology/service), distributed honeypots (for spam blocking), distributed power mass data storage service, email reputation service (technology/service), file reputation service (technology/service), firewalls (traditional security technique), IDS (intrusion detection system) (traditional security technique), intelligent analysis service of security log, intelligent mining service of security log, intelligent security analysis service, IPS (intrusion prevention system) (traditional security technique), relative analysis of behaviour service (technology/service), sample data collection service, sender reputation (for spam blocking), spam mail filtering (based on cloud security), threat detection (based on cloud security), threat detection system (based on cloud security), threat perception (for spam blocking), threat processing service, VPN (traditional security technique), web reputation service (technology/service), white list service (technology/service) |
| Vorakulpipat et al. (2014) | **Classifications:** Business-oriented perspective, Information security management system (ISMS) perspective<br><br>Consulting services, helpdesk services, network services, software development services |
| Xia & Hu (2006) | Algorithms, data encryption standard (DES) algorithm, RSA algorithm |

## APPENDIX 3.1 Survey cover note

DigiWars on täällä! Valtioneuvoston kanslia tarvitsee Sinua. Vastaa tietoturvapalvelujen käyttöä koskevaan kyselyyn.
Kiitos! Kysely: https://lnkd.in/e9X4vS2

## APPENDIX 3.2 Survey questionnaire

Turun yliopisto
University of Turku

### Kysely tietoturvapalveluista

Tämä kysely tutkii Suomessa toimivien yritysten tietoturvapalveluiden käyttöä. Kysely tehdään pro gradu -työhön osana Turun yliopiston ja Valtioneuvoston Digiwars-hanketta, jolla pyritään tukemaan digitalisaation hyödyntämistä liike-elämässä. Kyselyyn vastaaminen tapahtuu täysin anonyymisti ja luottamuksellisesti, eikä vastaajaa tai yritystä tulla yksilöimään tulosten perusteella. Kysely sisältää kaksi sivua; pakolliset kysymykset on merkitty tähdellä (*). Mikäli ette halua vastata johonkin pakolliseen tietoturva-aiheiseen monivalintakysymykseen, voitte valita vaihtoehdon 'en osaa sanoa'.

**Kyselyyn vastaaminen vie noin 5-10 minuuttia.** Muistattehan painaa kyselyn lopuksi Lähetä-painiketta; tällöin vastauksenne tallentuvat automaattisesti.

Kiitos vastauksistanne!

**Määritelkää roolinne yrityksessä.** *

- ○ Liiketoimintajohto
- ○ Liiketoiminnan asiantuntija
- ○ IT-johto
- ○ IT-asiantuntija
- ○ Tietoturvajohto
- ○ Tietoturva-asiantuntija
- ○ Jokin muu, mikä? _____

**Määritelkää yrityksenne toimiala.** *

- ○ Teollisuus ja kuljetus
- ○ Kauppa ja palvelut
- ○ Terveys ja hyvinvointi
- ○ Pankki- ja vakuutusala
- ○ IT ja viestintä
- ○ Julkishallinto ja puolustus
- ○ Energia ja vesi
- ○ Muut

**Määritelkää yrityksenne koko.** *

- ○ Alle 10 työntekijää
- ○ 10-49 työntekijää
- ○ 50-249 työntekijää
- ○ Yli 249 työntekijää

**Kuvailkaa omin sanoin, mitä ymmärrätte tietoturvapalvelulla tarkoitettavan.** *

_____

**Kuinka tärkeiksi arvioitte tietoturvapalvelut yleisesti organisaationne tietoturvan varmistamiselle?** *

- Ei lainkaan tärkeä
- Ei kovin tärkeä
- Ei tärkeä eikä tarpeeton
- Melko tärkeä
- Erittäin tärkeä
- En osaa sanoa

**Millaisia tietoturvapalveluita organisaationne käyttää ja mikä on eri tietoturvapalveluiden tärkeys organisaationne tietoturvan varmistamiselle?** *

Vastaattehan käytön ja tärkeyden jokaisen alla listatun palvelukategorian osalta.

*Käyttö*: Valitkaa tietoturvapalvelukategorian käyttöä vastaava vaihtoehto (ei käytössä, käytössä, en osaa sanoa).
*Tärkeys*: Arvioikaa palvelukategorian tärkeyttä (ei lainkaan tärkeä, ei kovin tärkeä, ei tärkeä eikä tarpeeton, melko tärkeä, erittäin tärkeä, en osaa sanoa).

| | Käyttö | | | | Tärkeys | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Ei käytössä | Käytössä | En osaa sanoa | | Ei lainkaan tärkeä | Ei kovin tärkeä | Ei tärkeä eikä tarpeeton | Melko tärkeä | Erittäin tärkeä | En osaa sanoa |
| **Fyysinen turvallisuus** (tietoturvapalvelut yrityksen fyysisen ja ympäristön turvallisuuden takaamiseen) | ○ | ○ | ○ | 1. | ○ | ○ | ○ | ○ | ○ | ○ |
| **Hallinnollinen turvallisuus** (tietoturvapalvelut tietoturvapolitiikan ja -toimintamallien noudattamiseen, kehittämiseen ja johtamiseen sisältäen sidosryhmähallinnan, tietosuojan ja sertifioinnit) | ○ | ○ | ○ | 2. | ○ | ○ | ○ | ○ | ○ | ○ |
| **Henkilöstöturvallisuus** (tietoturvapalvelut henkilöstön turvallisuuden ja tietoturvaosaamisen takaamiseen) | ○ | ○ | ○ | 3. | ○ | ○ | ○ | ○ | ○ | ○ |
| **Tietoaineistoturvallisuus** (tietoturvapalvelut yrityksen tietoaineiston hallintaan sisältäen esimerkiksi aineiston luokittelun, säilytyksen, varmistamisen, palauttamisen ja tuhoamisen) | ○ | ○ | ○ | 4. | ○ | ○ | ○ | ○ | ○ | ○ |
| **Ohjelmistoturvallisuus** (tietoturvapalvelut liittyen yrityksen ohjelmistojen tietoturvalliseen kehitykseen, testaukseen, ylläpitoon ja valvontaan) | ○ | ○ | ○ | 5. | ○ | ○ | ○ | ○ | ○ | ○ |
| **Laitteistoturvallisuus** (tietoturvapalvelut yrityksen tietojärjestelmiin kytkettyjen laitteistojen testaukseen, asennukseen, ylläpitoon, valvontaan, huoltoon, elinkaarenhallintaan ja käytöstä aiheutuvien vaaratekijöiden arviointiin) | ○ | ○ | ○ | 6. | ○ | ○ | ○ | ○ | ○ | ○ |
| **Tietoliikenneturvallisuus** (tietoturvapalvelut yrityksien tietoliikenneyhteyksien turvallisuuden takaamiseen, tietoliikenteen salaamiseen sekä tietoliikennelaitteiston ylläpitoon ja valvontaan) | ○ | ○ | ○ | 7. | ○ | ○ | ○ | ○ | ○ | ○ |
| **Käyttöturvallisuus** (tietoturvapalvelut liittyen yrityksen tietojärjestelmien analysointiin, auditointiin, ylläpitoon, valvontaan ja suojaukseen, jatkuvuuden ja käyttöoikeuksien hallintaan, käytön tukeen ja lokien valvontaan) | ○ | ○ | ○ | 8. | ○ | ○ | ○ | ○ | ○ | ○ |

**Mikäli organisaationne käytössä on muita kuin edellisiin kategorioihin sopivia tietoturvapalveluita, kirjatkaa ne alla oleviin kenttiin ja arvioikaa niiden tärkeys organisaationne tietoturvan varmistamiselle.**

| | | Tärkeys | | | | | |
|---|---|---|---|---|---|---|---|
| | | Ei lainkaan tärkeä | Ei kovin tärkeä | Ei tärkeä eikä tarpeeton | Melko tärkeä | Erittäin tärkeä | En osaa sanoa |
| Tietoturvapalvelu 1 | 1. | ○ | ○ | ○ | ○ | ○ | ○ |
| Tietoturvapalvelu 2 | 2. | ○ | ○ | ○ | ○ | ○ | ○ |
| Tietoturvapalvelu 3 | 3. | ○ | ○ | ○ | ○ | ○ | ○ |
| Tietoturvapalvelu 4 | 4. | ○ | ○ | ○ | ○ | ○ | ○ |
| Tietoturvapalvelu 5 | 5. | ○ | ○ | ○ | ○ | ○ | ○ |

**Millaisia tietoturvapalveluita käytätte tiedon a) luottamuksellisuuden, b) eheyden ja c) saatavuuden varmistamiseen?**

Kuvailkaa vapaasti.

Luottamuksellisuus

Eheys

Saatavuus

**Hyödynnättekö ulkoisia palveluntarjoajia organisaationne käyttämissä tietoturvapalveluissa?**
Kysely poimii tähän palvelukategoriat, jotka valitsitte aiemmin käytössä oleviksi. Mikäli ette valinneet yhtäkään palvelukategoriaa käytössä olevaksi, näkyy tämä kysymys tyhjänä ja voitte siirtyä suoraan seuraavaan kysymykseen.

**Fyysinen turvallisuus**

| | Ei ulkoistettu | Osittain ulkoistettu | Täysin ulkoistettu | En osaa sanoa |
|---|---|---|---|---|
| Ulkoistuksen taso | ○ | ○ | ○ | ○ |

**Hallinnollinen turvallisuus**

| | Ei ulkoistettu | Osittain ulkoistettu | Täysin ulkoistettu | En osaa sanoa |
|---|---|---|---|---|
| Ulkoistuksen taso | ○ | ○ | ○ | ○ |

**Henkilöstöturvallisuus**

| | Ei ulkoistettu | Osittain ulkoistettu | Täysin ulkoistettu | En osaa sanoa |
|---|---|---|---|---|
| Ulkoistuksen taso | ○ | ○ | ○ | ○ |

**Tietoaineistoturvallisuus**

| | Ei ulkoistettu | Osittain ulkoistettu | Täysin ulkoistettu | En osaa sanoa |
|---|---|---|---|---|
| Ulkoistuksen taso | ○ | ○ | ○ | ○ |

**Ohjelmistoturvallisuus**

| | Ei ulkoistettu | Osittain ulkoistettu | Täysin ulkoistettu | En osaa sanoa |
|---|---|---|---|---|
| Ulkoistuksen taso | ○ | ○ | ○ | ○ |

**Laitteistoturvallisuus**

| | Ei ulkoistettu | Osittain ulkoistettu | Täysin ulkoistettu | En osaa sanoa |
|---|---|---|---|---|
| Ulkoistuksen taso | ○ | ○ | ○ | ○ |

**Tietoliikenneturvallisuus**

| | Ei ulkoistettu | Osittain ulkoistettu | Täysin ulkoistettu | En osaa sanoa |
|---|---|---|---|---|
| Ulkoistuksen taso | ○ | ○ | ○ | ○ |

**Käyttöturvallisuus**

| | Ei ulkoistettu | Osittain ulkoistettu | Täysin ulkoistettu | En osaa sanoa |
|---|---|---|---|---|
| Ulkoistuksen taso | ○ | ○ | ○ | ○ |

**Mikäli organisaationne hyödyntää ulkopuolisia palveluntarjoajia tietoturvapalveluihin, mitkä ovat olleet tärkeimmät syyt ulkoistukseen?**
Voitte valita useita vaihtoehtoja.

- ☐ Kustannustehokkuus ja/tai tarve säästää tietoturvakustannuksissa
- ☐ Tarve laaja-alaisemmalle tietoturvaosaamiselle ja -kokemukselle
- ☐ Tarve joustaville ja skaalautuville tietoturvaresursseille tai -palveluille
- ☐ Organisaation oman tietoturvaosaamisen puutteellisuus
- ☐ Organisaation omien tietoturvaresurssien riittämättömyys
- ☐ Halu keskittyä organisaation ydinosaamiseen
- ☐ Tietoturvapalveluiden parempi hallinta (esim. keskittämisen kautta)
- ☐ Laki, asiakas tai jokin muu taho vaatii (esim. auditoinnit ja sertifioinnit)
- ☐ Muu syy, mikä?

**Millaiseksi arvioisitte organisaationne tietoturvaosaamisen?** *

- ○ Erittäin huonolla tasolla
- ○ Melko huonolla tasolla
- ○ Ei hyvällä eikä huonolla tasolla
- ○ Melko hyvällä tasolla
- ○ Erittäin hyvällä tasolla
- ○ En osaa sanoa

**Millaisia tarpeita organisaatiollanne on tietoturvapalveluiden ja niihin liittyvän osaamisen osalta?**
Kuvailkaa vapaasti.

Tietoturvapalvelut

Tietoturvapalveluihin liittyvä osaaminen

**Miten ajattelitte vastata organisaationne tarpeisiin tietoturvapalveluiden ja niihin liittyvän osaamisen osalta?**
Kuvailkaa vapaasti.

Tietoturvapalvelut

Tietoturvapalveluihin liittyvä osaaminen

**Miten paljon organisaationne aikoo investoida tietoturvapalveluihin seuraavan 12 kuukauden aikana verrattuna aiempaan?** *

- Huomattavasti vähemmän
- Jonkin verran vähemmän
- Saman verran kuin aiemmin
- Jonkin verran enemmän
- Huomattavasti enemmän
- En osaa sanoa

**Tässä voitte antaa palautetta ja kommentteja kyselyyn ja sen kysymyksiin liittyen.**

Vastauksenne ovat nyt tallentuneet ja ne käsitellään ehdottoman luottamuksellisesti.
Voitte sulkea selaimen.

Kiitos osallistumisestanne!