Building inter-organizational trust by implementing information security management system – a review from trust building perspective
Abstract

Inter-organisational trust is increasingly important among supply chain participants, where threats are building up from sources out of organisational control. The same problem is faced in the cyber security field, where threat level increases from the changes outside organisational boundaries. Each value chain participating in the supply chain must be secured. Trust building is mandated among all trust network members. The business interaction between supply chain participants is enabled by building inter-organisational trust first. This study provided ways to build this inter-organisational trust by considering steps to take in information security management system (ISMS) implementation.

ISMS is set of processes, documentation, activities and resources that together secure assets within an organisation. It must be assembled to support strategic business goals and comply selected requirement criteria. Due to different ways and purposes, organisations implement ISMS’s and obtain the security standard certification; it is not a proof of secure business processes or trust per se. Instead, it is a good starting point for trust building.

This study used narrative literature review to find supporting and resisting elements of inter-organisational trust that can consider in ISMS. The study limited the research into a very narrow area between information processing science, behaviour sciences and discipline of management. The research found several elements (102) that can be considered in ISMS to have the effect to inter-organisational trust building. The findings were categorised using ISO/IEC 27001 (2013) ISMS implementation steps to provide concrete support for security professionals.

There are none or very limited number of research literature on exact combined topic of inter-organisational trust building and ISMS. The multidisciplinary phenomenon of information security coupled with inter-organisational trust requires more attention from the research community. Schools teaching information security should develop their course coverage to support this multidisciplinary phenomenon in several view points, not just from their own discipline to achieve producing suitable resources for the industry.

Keywords

trust, inter-organisational trust, trust building, information security management system, ISMS

Supervisor

Ph.D., Raija Halonen
Foreword

This study was hard, but still an enjoyable journey of learning. It all started from formulating ISMS core components and abandoning the dominant perspective how it was described in science. After I run into a research paper from Ph.D. Mikko Siponen considering errors in standards I started to question standards as a whole. I tried to start from a scratch to see how ISMS components were sourced in research, and how they magically appeared in standards used to cover ISMSs. It was path too unclear and hard to follow. I had to start all over again. Sorry, Mari and Raija! I needed to find a new research topic that would support my current career path and interests at the same time. Trust was found in a meeting with Mari. The old thesis was reformed and restarted from entirely new groundings.

This study was a fight against time and scientific research targets all to the bitter end. I actually believe, that I learned a lot from this study and hoped someone would also learn something new. I am happy to see that despite the pressure raised over completing my studies, my values are still intact. It is important to realise your values, and this journey helped me to accomplish this. I hope everyone would have this kind of opportunity to test them!

I thank my employer (Bittium) for letting me out-of-office so fluently, my supervisor Ph.D. Raija Halonen and opponent Ph.D. Mari Karjalainen to get my thesis text back in-line. Moreover, I thank my family for understanding the enormous pressure to finalise my studies. As Mr Kotter and his penguins taught me “change starts from the sense of urgency”. With this thesis, it is now once again empirically proved.

Thanks also go to my study friends Pekka and Jouko. You are the best! Thank you, big brother, for cheering me during my studies. Finally, I send my love to my family; Tuija, Siiri, Seela and Saimi for all the support you gave. Thank you for pulling me back to the real world of play and love when I opened the front door at home.

Karri Maijanen

Oulu, November 25th, 2016
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC</td>
<td>the International Electrotechnical Commission</td>
</tr>
<tr>
<td>ISA</td>
<td>Information Security Architecture</td>
</tr>
<tr>
<td>ISM</td>
<td>Information Security Management (ISO/IEC 27001, 2013)</td>
</tr>
<tr>
<td>ISO</td>
<td>the International Organization for Standardization</td>
</tr>
</tbody>
</table>
# Contents

Abstract ................................................................................................................................................. 2  
Foreword .................................................................................................................................................. 3  
Abbreviations ......................................................................................................................................... 4  
Contents .................................................................................................................................................... 5  
1. Introduction .......................................................................................................................................... 6  
2. Key concepts ......................................................................................................................................... 10  
   2.1 Inter-organisational trust ..................................................................................................................... 10  
   2.2 Information security management system (ISMS) .............................................................................. 13  
   2.3 ISMS implementation steps ................................................................................................................ 18  
3. Research Methods ............................................................................................................................ 21  
   3.1 Narrative literature overview ............................................................................................................. 21  
   3.2 Application of research method ........................................................................................................ 24  
4. Elements affecting inter-organisational trust .................................................................................... 28  
   4.1.1 Obtaining management approval for initiating an ISMS project ..................................................... 28  
   4.1.2 Defining ISMS scope, boundaries and ISMS policy ................................................................. 33  
   4.1.3 Conducting information security requirements analysis ............................................................ 36  
   4.1.4 Conducting risk assessment and planning risk treatment ............................................................ 37  
   4.1.5 Designing the ISMS ....................................................................................................................... 38  
5. Discussion and implications .............................................................................................................. 40  
6. Conclusions .......................................................................................................................................... 42  
References ................................................................................................................................................. 45  
Appendix 1 References for inter-organisational trust ............................................................................. 50  
Appendix 2 References for describing key concepts ............................................................................ 52
1. Introduction

The purpose of this study was to find the supporting and resisting elements of inter-organisational trust that can be achieved by implementing information security management system (ISMS). As Porvari (2012) explained, information security is a multidisciplinary phenomenon. This study concentrated on research papers of inter-organisational trust from information, behaviour and management sciences under the selected topic. Trust building among stakeholders is one of the benefits why companies are implementing ISMSs (ISO/IEC 27000, 2016; Järveläinen, 2012). Trust is also a key factor and one of the main enablers in business co-operation (Castelfranchi, 2008; de Oliveira Albuquerque, García Villalba, Sandoval Orozco, Buiati, & Kim, 2014; Dyer & Chu, 2011; Seppänen, Blomqvist, & Sundqvist, 2007). Implementing ISMS will also benefit business to limit information security risk effects (ISO/IEC 27000, 2016).

Business objectives are linked to ISMS and trust by managing risks and developing trust (de Oliveira Albuquerque et al., 2014). Sourcing these trust affecting items from the research supports trust building between companies. Trust is required to co-operate in a way that vulnerabilities of the business are exposed. Since trust building will enable co-operation and other’s vulnerabilities are easier to exploit, the trust must be built before co-operation can deepen and confidential or business critical information can be shared (Barney & Hansen, 1994). Cooperation requires the exchange of knowledge across organisational boundaries, and it demands trust (Vélez, Sánchez, & Álvarez-Dardet, 2008; Zhang, 2011). Trust directs partnering organisations to maintain sufficient security level by controls it enables (Barney & Hansen, 1994). To successfully implement information security at the corporate level you need to understand the multidisciplinary phenomenon and have knowledge on a wide set of disciplines (Porvari, 2012).

In prior research, there are several studies on trust in business and why inter-organisational trust is a requirement starting business co-operation. It was also found that there are none or very limited number of research papers found from the specific conjunction of ISMS and inter-organisational trust building. Trust building matters in the context of inter-organisational relationships (Castelfranchi, 2008; de Oliveira Albuquerque et al., 2014; Seppänen et al., 2007). According to Seppänen et al. (2007), trust is required to be constructed before organisations are willing to exchange confidential or critical business information, communicate openly and sort conflicts efficiently. Therefore trust is an essential building block in business crossing organisational boundaries. Business operations inside a supply chain must be able to develop predictability, resilience and fit in new business situations (Seppänen et al., 2007). Competition in global markets raises chain flexibility into an important role, and this flexibility can be achieved by utilising inter-organisational trust (Zhao, Ling, & Xu, 2010). According to Seppänen et al. (2007), these goals are accomplished with inter-organisational trust among supply chain participants. Trust is about actively giving another business partner to deal with vulnerabilities of one’s business (Mayer, Davis, & Schoorman, 1995). The benefits of partnership and similarly of trust are seen as being more resilient through collaboration, easier adaptation to changes in business environment and being more predictable (Seppänen et al., 2007). As opposing force collaboration without trust can also be considered (MacDuffie, 2011).
The concept of trust and level of subjectively measurable inter-organisational trust varies even among different countries and cultures (Hexmoor, Wilson, & Bhattaram, 2006; Seppänen et al., 2007; Zucker, 1987). Between organisations financial limitations, nature of communication and shared values favour trust building and dependence resist it (Seppänen et al., 2007; Young-Ybarra & Wiersema, 1999). Trust is bound to organisational elements such as processes, teamwork and collaboration (Dyer & Chu, 2011; Hexmoor et al., 2006). Trust is also felt to be the result of shared values and known identification (Savolainen, 2008; Seppänen et al., 2007; Zucker, 1987).

Trust is investigated from sociological and embeddedness, process and economic perspective where organisational elements draw trust from individual level and effects to this are analysed from an economic standpoint (Dyer & Chu, 2011). A number of trust-based security models were developed to investigate and analyse effects of found trust elements among individual trust and inter-organisational trust (de Oliveira Albuquerque et al., 2014; de Oliveira Albuquerque, García Villalba, Sandoval Orozco, de Sousa Júnior, & Kim, 2015; Hexmoor et al., 2006).

ISMS should be generated first and then verify it is holistic implementation using selected criteria to reach best protection level suited to the business at hand (Eloff & Eloff, 2005). Security criteria should be used as a checklist, not the only security work and implementation feeding source, for information security specialists to verify that all security perspectives are implemented into ISMS (Siponen & Willison, 2009). ISMS sourced from a standard should also be enhancing the quality of business processes instead of merely supporting the existence of a required processes (Siponen, 2006).

The study of inter-organisational trust in this paper was limited to trust phenomenon only between companies, not between institutions, organisations and customers, or people inside a company or a group. This study limited research to the concept of trust only in information security part of inter-organisational trust building and implicitly to considerations on implementing an ISMS.

The study was also restricted to be using narrative literature review as an information source. This approach was found relevant to point out a research gap found at the exact research topic of this study; ISMS and how inter-organisational trust building can be affected in implementing it. Due to the research gap discovered in this study, there was not identified exactly matching research papers on elements related to inter-organisational trust in ISMS implementation. Therefore, these elements affecting inter-organisational trust are retrieved from research papers surrounding the topic and present one limitation in this research.

The selection of articles employed in this study was limited only to those that considered inter-organisational trust or information security and which the University of Oulu had full text access through Scopus search engine or the paper was publicly accessible using Google Scholar search. All books were also removed from results, and only articles, reviews and conference papers were included. Language approved into the research were only English or Finnish. Retracted papers were also excluded from the study.

Another limitation of this study was applied research method in phase 1 literature review could have been accomplished with strict search words and research paper selection. Due to this, the concepts defined in the chapters 2.1 and 2.2 were not following narrative literature review rigorously as described in Chapter 3.1.
Very restricted search words were used in this study. By leveraging variable word list such as “inter-organizational”, “inter-organisational”, “interorganisational”, “interorganizational” and “inter-firm” combined to targeting search also into Abstract and Keywords would have resulted in the higher number of research papers.

The research question of this study was “How to support inter-organisational trust by ISMS implementation?”. Implementing ISMS was placed at the centre of the study. Inter-organisational trust effecting elements were retrieved from the literature with the narrative literature review. Finally, these elements were categorised and analysed to reveal trust support engaged in different phases of implementing ISMS. Articles were limited only to those who had coverage on ISMS or inter-organisational trust since research papers related to ISMS, and inter-organisational trust was not found.

This study used narrative literature review to find affecting elements of inter-organisational trust building. These elements can support or resist inter-organisational trust building. Since the area of trust combined with ISMS is very broad, the study was limited only to find these supporting and resisting elements in inter-organisational trust related to security implementations of ISMS.

Already preliminary literature research resulted, that ISMS-related trust building was not researched thoroughly. ISMS and inter-organisational trust research should consider at least three different disciplines such as administrative, behavioural and informational sciences. There were none or very limited number of research papers found from this specific conjunction of sciences and research topic of ISMS and inter-organisational trust building.

This study started filling this research gap between trust and implementation of ISMS. This study extracted elements that can help building inter-organisational trust and categorising them into ISO/IEC 27003 (2010) ISMS implementation steps to help information security specialists and managers to understand how the implementation of ISMS can have the effect to trust. This study also revealed that ISMS and trust should be explored together, but since they are presented in different disciplines as in administrative, behaviour and information science it is rarely available in any single school’s curriculum.

The study limited the research into a very narrow area between information processing science, behaviour sciences and discipline of management. As information security is multidisciplinary phenomenon, knowledge from all of these areas are required to be a successful implementer of information security in corporate level (Porvari, 2012).
The research gap was found already in the preliminary literature research, and it is opened up in Picture 1. It was found in multidisciplinary conjunction of information science, administrative science and behavioural science. During preliminary literature research, it was already found that in the combination of inter-organisational trust and ISMS implementation, these topics were not well enough studied together to support decision making in trust building.

The study is structured into six chapters. From top-down, Chapter 1 introduces the study to the reader. Chapter 2 introduces the key concepts. Chapter 3 explains research method applied, followed by Chapter 4 presenting the findings. After that Chapter 5 discusses the results comparing them to the previous research. Chapter 6 concluded the research and proposed new research topics from the focus area of the study.
2. Key concepts

Since the study did not find any exact research papers, this chapter provided knowledge about surrounding key concepts. In Chapter 2.1 trust and inter-organisational trust concept were opened. In Chapter 2.2, ISMS was extracted from information security management (ISM) by defining the concept. In Chapter 2.3, the steps of implementing an ISMS were explained. These key concepts were required to be understood in search for supporting and resisting elements from the interconnection of inter-organisational trust and ISMS implementation. These supporting and resisting inter-organisational trust elements were then explained thoroughly in Chapter 4 as results.

2.1 Inter-organisational trust

Trust is not easily explained (Savolainen, 2008; Zaheer, McEvily, & Perrone, 1998). It is a positive thing (Hexmoor et al., 2006). It can be defined as “willingness to be vulnerable”, and it is risk taking inherently by choosing to be vulnerable (Mayer et al., 1995, p.724). It is confidence within supply chain participants that vulnerabilities opened will not be exploited by any participating organisation (Barney & Hansen, 1994). In this case, the vulnerability is something organisations are willing to take when the trust is established (Dyer & Chu, 2011). It is not self-evident that this risk is wanted, but it has to be taken to proceed example in business co-operation over supply chains (Barney & Hansen, 1994). Without trust, there are significant difficulties to do business (Zaheer et al., 1998). The level of trust between organisations and simultaneously risk taking level defines the controls against opportunism required (Hexmoor et al., 2006). This opportunism risk is valued between trustee and trustor organisations. Cost and benefit analysis related to controls defines the level of trust organisations are willing to pledge (Dyer & Chu, 2011; Hexmoor et al., 2006).

Behaviour of others in actions predictability and confidence in goodwill is another definition of trust (Zaheer et al., 1998). According to Zhang (2011), goodwill is having a positive effect on relational risk on partnerships. Albuquerque et al. (2014) define trust as probability things keep on going as they are supposed to. This refers to the continuity of something already agreed and assumes trust will be preserved. Trust constructs on a personal level as an assessment of trustworthiness and benevolence by representing positive expectations and behaving respectfully also in opportunistic situations (Savolainen, 2008). Vulnerability, risk and positive expectations are core pieces of trust (Hexmoor et al., 2006; Savolainen, 2008).

As several definitions were presented in this chapter, trust can be explained many ways (Savolainen, 2008). Trust concept also varies from the level it is observed (Rousseau, Sitkin, Burt, & Camerer, 1998). There is no generally accepted concept of trust among researchers (Savolainen, 2008).
The multidimensional concept of trust is presented in Picture 2. Seppänen et al. (2007) listed trust dimensions to reveal how forming the definition of trust is difficult. Trust is not defined properly in literature (Seppänen et al., 2007). Trust is a phenomenon experienced individually by value perception (Seppänen et al., 2007).

In a simplified view, within economics, trust is seen as receiving reciprocation in Castelfranchi’s (2008) multi-layer cognitive model, where trust is not only perceived as attitude towards trustee but confidence that makes truster vulnerable and dependent in business exchange. Trust in business exchange is the probability that it will be completed in good faith (Zucker, 1987). Trust has effects on business performance through exchange performance (Zaheer et al., 1998). Trustworthy is also experienced as a competitive advantage, which benefits business greatly if it is available only for few organisations (Barney & Hansen, 1994).

Assumptions between economically and behaviorally oriented research groups are mainly different. Economics present world without the assumption of trust and trust can be achieved by making binding contracts in varying levels (Barney & Hansen, 1994). Behaviour science is emphasising trust in exchange by who or what partners are (Barney & Hansen, 1994). Economics observed that it is also tough to distinguish whether exchange partner can be trusted or not (Barney & Hansen, 1994).

Between organisations nature of communication openness and shared values favour trust building. Dependence depth is negatively affecting to it. Open communication is also building trust. Shared values are having a positive effect on trust. Dependency mainly affecting decision making is negatively affecting trust between organisations. (Young-Ybarra & Wiersema, 1999.)

Inter-organisational business studies explain trust in two different ways: first is predictability and confidence in the behaviour of other and other is benevolence through confidence (Dyer & Chu, 2011). Another viewpoint is that in inter-organisational relationships vulnerabilities are exposed, but still those are not exploited due to trust (Barney & Hansen, 1994). According to Barney and Hansen (1994), opportunism is a
negation of trust. This is easily seen, when trust is opening vulnerabilities in business exchange.

Trust is essential for success, and it is also required to create products beyond own organisational borders. Trust supports more open conflict handling, communication and information sharing. These factors are important to develop functional business relationships. (Seppänen et al., 2007.)

Trust can also be explained as: “Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another” (Rousseau et al., 1998, p.395). Rousseau et al. (1998) state psychological perspective of trust to be the intention for good, and it can be seen as intentions or behaviour of another party. Trust is only partly psychology as in micro level. The trust’s psychological perspective is expanded into multiple layers by broadening the scope of trust. These levels are opened in Picture 3. (Rousseau et al., 1998.)

![Picture 3](Levels of trust according to Rousseau et al. (1998)).

As stated in Picture 3 there are several levels of trust. In between each level, different core objects create the diversity of trust so that each level differs in the way trust is defined in it (Rousseau et al., 1998). Varying levels of trust make trust also more complicated and therefore, trust is harder to explain or define (Rousseau et al., 1998). Trust is a willingness to fulfil obligations, reliability, predictability and fairness (Zaheer et al., 1998). Trust is a multi-level phenomenon, and even today it seems there is no clear agreement of definition among researchers. Trust is an individual level concept, but effects to inter-organisational performance (Dyer & Chu, 2011; Zaheer et al., 1998). The individual level of trust is sourced from behaviour and intentions, and Zaheer et al. (1998) explained the level to be a combination of following core objects: Negotiation, conflict and performance. Individual level trust is related to personal level trust and can be seen as lowered negotiation costs, but does not have an effect on conflict costs. In group-level of trust is bound to actions taken in co-operation. The group delivers the same level of trust to co-operation partners as individual members. (Zaheer et al., 1998.)

In the inter-organisational level, the trust has broader coverage than in individual or group level, and it is placed into partnering organisation by trusting organisation. Trust in supply chains is an inter-organisational level of trust. It spreads the assumptions of partner actions between all organisations participating in the network of trust. Inter-organisational trust has direct effects on lowered negotiation and conflict costs. Inter-organisational trust effects are therefore part of cooperative actions between organisations. (Zaheer et al., 1998.)

The last level is an Institutional level of trust. It is trust towards countries, and it is based on implicit trust bound to a society built on the institutional environment (Dyer & Chu, 2011). Higher trust towards society, the higher ability it has to compete (Dyer & Chu, 2011).
2.2 Information security management system (ISMS)

As Porvari (2012) explained, information security is a multidisciplinary and new phenomenon and when discussed information security, meanings of commonly used concepts differs among people. Proper ISM is a joint effort of supporting organisational culture, intelligent technology and supportive attitude toward IS by management (Chang & Lin, 2007). These areas can be addressed by running a management system, especially when running an ISMS system. Different disciplines related to information security are listed in Picture 4.

![Disciplines related to information security (Porvari, 2012).](image)

Multidisciplinary of information security is visualised in Picture 4. According to Porvari (2012), multidisciplinary of information security can be divided into six different areas. Business risks are managed with the help of economics. Administrative Sciences describe security management, its organisations, and risk management processes. Behavioural Sciences explain employee behaviour and link organisational culture closely into information security. Human behaviour is inflected by social psychology, sociology, and psychology. This information can be used on effective security awareness programs. Analysis of security and risks are based on probability and statistics. Security controls can also contain technology and information systems so they can also be drawn to be information processing science. (Porvari, 2012.)

Information security is a multidisciplinary phenomenon, and it must be implemented everywhere to be a success. Bad choices in human resources can have a disastrous effect on the ethics of employees and lower employee’s morale to compromise security. The human factor cannot be diminished when developing information security. Properly adjusted ISM must take properly into consideration of risks related to humans. (Eloff & Eloff, 2005.)

Information security is a central concern of the whole organisation (Firoiu, 2015). The concept of ISM varies in between researchers and institutions (Hong, Chi, Chao, & Tang, 2003). As Eloff & Eloff (2005) structured, architecturally ISM is complex and expensive to implement into organisations since improper or inefficient implementation will also be costly in the shape of a security breach. This leads to that; ISM is a multidimensional process, and information security architecture (ISA) was presented to help follow it through. The more varied IT environment is, the more difficult it is to secure (Ross, 2008). ISA supports the holistic implementation of information security
into organisations. ISA is a way to ensure all objects know their relations between each other. Awareness also means that personnel knows their responsibilities and know how to work secure way. ISA can be divided into five different aspects, which are opened in Picture 5. (Eloff & Eloff, 2005.)

In Picture 5 ISA is explained through ISM functionalities. Together these five parts are forming ISMS main areas. Security organisation and infrastructure are the personnel and platform for executing ISMS. Security policies, standards and procedures are results of analysis of security should be implemented within the organisation. Security program opens up controls and reveals risks they are controlling. Security culture awareness and training program is explaining those methods how information security is going to be sold to personnel. Finally, compliance is monitored, and feedback will be fed back to the beginning of the cycle. (Eloff & Eloff, 2005.)

IT structures, organisations, environment, and business all changes. These changes must be managed properly to enable efficient ISM. ISA delivers information of all parts there must be considered within an ISMS. New phenomenon’s in technological advancement has an effect also to the security posture of the business environment. Even within an organisation, there are changes to be met with the ever-increasing complexity. (Eloff & Eloff, 2005.)

When designing ISMS at the end of the development process pipe, there are controls, which tries to define wanted actions toward the desired level of security. Controls are intertwined together as one big network of relations. Relations must be brought up to see total effect of connected controls within ISMS. ISA will help the designer and implementer to identify these links. (Eloff & Eloff, 2005.)

According to Von Solms (1998) in ISO/IEC 17799:1993 ISM is divided into ten categories. Categories divide different parts of ISM into a list of functions, that later on are transferred into implementation steps in (ISO/IEC 27001, 2013). These categories are listed in Picture 6.
Categories are opened in **Picture 6**. In the picture, each box represents separate ISM categories. *Information security policy* is explaining target level of information security within the organisation. The policy is the security documentation of the organisation. It also delivers hands-on information regarding how to work in a secure way and how to comply security requirements. This documentation needs to be regularly assessed to make sure it is compliant with changes in business environment. *Information organisation and their responsibilities* must be known to all employees. Everyone must understand things he or she are not allowed to do and what responsibilities he or she have over information security. It is part of awareness, which is explained in detail in personnel security management and training. (Von Solms, 1998.)

*Information assets security management, classification, and control* box in **Picture 6** contains risk management perspective of information security and it determines assets, classifies them, and defines security controls to protect them (Von Solms, 1998). The asset is the heart of information security, and risk management is the process to protect it (Breier & Schindler, 2014). Information security provides means to protect assets in methods of risk management (Blakley, McDermott, & Geer, 2001). *Personnel security management and training* is providing controls to personnel security, where technology is having problems to achieve required results (Chang & Lin, 2007). Methods to control risk through awareness are most valuable for the organisation since threats related to personnel are largest there is (Siponen, Pahnila, & Mahmood, 2010).

The effectiveness of information security is based on the holistic implementation in all parts of the organisation and broader influence there is, the better protection is accomplished (Eloff & Eloff, 2005). This thought is supported by *Physical and environmental security management*, which secures physical world around assets. Physical layers are the concrete thing one can touch. This convergence of physical security and information security can enhance the overall level of security (Kang & Kim, 2015). While assets lie around information systems, they are part of *computer and network system security management*, and this function will protect assets located inside information systems (Von Solms, 1998).

*System access control* protects assets inside the information system against unauthorised access and it defines what user and software can do inside an IT system (Poniszewska-Maranda, 2006). IT systems changing and improving all the time there is a need to
System development and maintenance security management. This function will keep systems up-to-date and makes them better suited for securing assets inside them. Business contingency planning tries to ensure business processes can continue without interruption even in a crisis situation. The final category is Compliance. It is about reporting the status of information security within the organisation and how policy is followed. It serves as visibility view towards ISM for top-management. (Von Solms, 1998.)

As Morling and Tanner (2000) explains there are many kinds of management systems within a company. These systems purpose is to help the organisation to reach its goals and these management systems support organisation to control activities and resources that are required to achieve organisational targets (Morling & Tanner, 2000). The management system is a group of factors inside the organisation to set up objectives, policies and processes to achieve defined goals of organisational existence (ISO/IEC 27000, 2016).

The management system is essential for the business (Morling & Tanner, 2000). To enable and enhance management systems two management model cycles are used. These management model cycles are introduced in Picture 7 and Picture 8. The cycles are PDCA- and DMAIC -model cycles. These models present the best practice within the organisation functions to achieve organisational goals. (Eloff & Eloff, 2005.)

PDCA cycle is explained in plain in Picture 7. It divides actions into four different parts to create an infinite loop of development actions and according to ISO/IEC 27000 – series, Plan-Do-Check-Act (PDCA) is presented as grounding cycle of all ISMS activities in the older 2005 version. Currently, PDCA model is removed from the standard (ISO/IEC 27001, 2013) and systematic approach, presented in Picture 10 is used instead. This cycle model attempted to enable, document, reinforce and improve best practices within the organisation. (Eloff & Eloff, 2005.)

Picture 7 PDCA cycle model (Eloff & Eloff, 2005).

Picture 8 DMAIC cycle model (Montgomery, 2010).
Another improvement cycle is presented in Picture 8. This enhancement cycle is called Design-Measure-Analyse-Improve-Control (DMAIC), and it is defined by Six Sigma. This cycle is more suitable for organisations which have defined their processes based on Six Sigma framework. Focus of Six Sigma is limiting variability to reach a minimum level of defects. This cycle is also driving towards operational excellence. (Montgomery, 2010.)

Both improvement cycles push towards better processes since the purpose is to manage change (Morling & Tanner, 2000). New model to push ISMS forward is presented in latest ISO/IEC 27001 (2013) standard as a systematic approach. This approach also reveals pathway towards the future through incremental improvement. All models indicate that change is required, but the amount of change per cycle can be minimal to keep it easily under control. Changes need to be seen as a cycle of activities. This way a process can be regarded as an ever-changing activity. On every cycle, this activity can be improved to take stakeholder environment changes into account. (Morling & Tanner, 2000.)

ISM was found a very complex task (Eloff & Eloff, 2005; Porvari, 2012). Now that the concept of ISM was explained, this paper continues towards ISMS, which was defined in ISO/IEC 27000 (2016) as the implementation of ISM enabled running within an organisation’s management system. The concept of ISMS has tried to be explained in security standards such as ISO/IEC 27000-series (ISO/IEC 27001, 2013).

As Eloff & Eloff (2005) explains that ISMS is architecturally complex and expensive to create, operate, and it can be grounded wrong way into the organisation to even lower security status. Creating ISMS is a very complex process, and it must be conducted in the holistic and well-structured way (Eloff & Eloff, 2005). The purpose of ISMS is to protect information resources by documenting intent into the policy and procedures (Ross, 2008). Implemented technology also represent commitment and together with them all; policy, procedures and technology forms the core components of ISMS (Ross, 2008).

As Picture 9 states, ISMS defined in ISO/IEC 27000 (2016) comprises organisational policies, procedures, guidelines, resources and activities to protect organisation’s...
information assets. The asset is drawn in Picture 10 into the middle, to be protected by outer items. As ISO/IEC 27000 (2016) express, ISMS is making information security better for business to flourish and its objectives to be reached by protecting assets.

![Picture 10](image10.png) ISMS steps opened as a systematic approach according to ISO/IEC 27000 (2016).

As Picture 10 indicated ISMS is the systematic procedure to “establish, implement, operate, monitor, review, maintain and improve information security” (ISO/IEC 27000, 2016, p.14). Presented operational steps help asset analysis and implementing controls to protect them. This systematic approach is considered as the new improvement model for ISMS, and it divides procedure steps into separate steps (ISO/IEC 27000, 2016).

2.3 ISMS implementation steps

This chapter opened the third important concept of this study: ISMS implementation steps. These steps were required to be understood, to support inter-organisational trust-building element categorising used in this study. In this study, it was chosen to categorise inter-organisational trust effecting elements into ISMS implementation steps to achieve simplicity. For information security professional this categorisation placed the affecting trust elements into broadly understood steps for easier understanding. According to Beckers (2014), ISMS defined in ISO/IEC 27001 (2013) can be established by the goal-oriented approach. These goal-oriented steps are explained in Picture 11.

![Picture 11](image11.png) ISMS implementation steps (Beckers, 2014).
In Picture 11 ISMS implementation steps are listed. ISMS implementation project begins by obtaining commitment and resources from the management level. Without decent resources, there is not going to be able to create a proper ISMS at the end. Resources are defined as roles and actors to accomplish ISMS. During the creation of ISMS, the commitment is required to be refreshed periodically. Commitment refreshing is needed due to the nature of rapid change in system implementations. (Beckers, 2014.)

ISO/IEC 27001 (2013) standard advice to understand the organisation, needs and expectations of stakeholders and to comprehend how organisation interact with other organisations. In this step, there should be defined the scope of ISMS implementation. ISMS scope boundaries can be defined to be as a company or function boundaries. They need to be exact and understandable by the organisation. The extent of the implementation can change and then it must be reviewed again by the management. Exceptions on selected scope must also be explained clearly. (Beckers, 2014.)

Scope definition will limit ISMS coverage into something concrete for asset analysis, which is the next step. Since all rest of the steps of ISMS implementation are based on scope definition, that step must be explained in a way that it is understood easily and can be communicated fluently. One way to define scope would be using a picture or process descriptions of all the processes within the scope. It needs to be consistent, clear and extensive. When the scope is explained in an easy way, then it can be understood by relevant stakeholders for proper and extensive asset discovery. (Beckers, 2014.)

Assets are protected by adequate security controls, and it is the purpose of ISO/IEC 27003 (2010) ISMS. Assets are defined to be anything with some value to the business. Assets must be identified so that they can be protected. This is stated in Picture 11 in step 3. After the asset is identified, threats related to its existence are listed and analysed on step 4. The analysis is covering threats, risks and impacts from a perspective of assets. (Beckers, 2014.)

Risks and vulnerabilities related to exploit of threats are listed. This information is compiled in risk analysis which is step 5 in Picture 11. Risk analysis produces a list of risks associated with each asset, and these risks need to be controlled. Security controls are used to limit adverse effects of risks within the organisation. If risk level is not acceptable, then security controls need to be chosen to diminish it. The last step is designing ISMS specification as documentation. This is explained in step 6. This step is documenting used management system in level, where document components can be discussed and analysed further. (Beckers, 2014.)

Beckers (2014) used ISO/IEC 27001 (2005) standard and steps to establish ISMS are updated in newer ISO/IEC 27003 (2010). Standard cut steps into 5 phases. These phases are listed in Picture 12 as ISMS project phases.
As stated in Picture 12 the number of steps were reduced from six to five implementation phases in the latest ISO/IEC 27003 (2010) standard and the content was also changed. Changes can be found in step 3, where previously assets were identified. New information security requirements analysis is also covering asset identification, and further information security assessment is conducted in that same phase. The rest of the implementation is unchanged. (ISO/IEC 27003, 2010.)
3. Research Methods

This chapter introduced the research approach to the reader. First, the research method narrative literature overview was explained. Second, the application of the chosen research method was reported. This opened the application of selected research method and the scope of application for the reader to understand how the original method was followed in the study.

The focus of this study was to retrieve elements affecting trust in ISMS implementation. These elements were searched from research papers covering the topic of inter-organisational trust. Research question “How to support inter-organisational trust by ISMS implementation?” defines the scope of the research into ISMS implementation, where elements affecting trust are retrieved using narrative literature overview. Elements are listed in Chapter 4 pictures and explained in the text following it. The research question is formulated to narrow the scope of the research into trust effecting elements research and categorising them by ISMS implementation steps.

3.1 Narrative literature overview

Literature research is a round-up of prior research. It gathers related research papers into the single analysis to enable easier result finding. Literature research is a critical study of contributions of previous research papers. It also opens up results and crystallises new perspectives on these research papers. (Rowe, 2014.)

Review of the literature is research method where current knowledge is reported from the limited scope (Green, Johnson, & Adams, 2006). It is a summary where previous research is combined with a new perspective. It also helps the reader to understand existing knowledge and giving it a fresh perspective within the limitations of the research. All data is retrieved from previous research papers. Literature research can be defined as a hierarchy of research types, which are listed in Picture 13. (Green et al., 2006.)
As Picture 13 explains literature research is divided into three different kinds of main types: “narrative review, qualitative systematic reviews, and quantitative systematic reviews” (Green et al., 2006, p.102-103). A narrative literature review is divided into three different kinds of sub-types: “editorials, commentaries and overview articles” (Green et al., 2006, p.103). The phase three of this study, which is explained in Picture 16, complies with the narrative overview. This method can also be called as “unsystematic narrative review” (Green et al., 2006, p.103).

The good narrative literature review should report information by using narrative review elements and structure, combine information sourced from previous research, respect limits of the research and indicate a clear message. Narrative literature review steps are defined in Picture 14. (Green et al., 2006.)

In Picture 14, the steps for writing narrative literature review are presented according to Green et al. (2006). The research starts from preliminary research, where current knowledge is studied. It must be verified, that topic of the present study is not already researched, and there is a gap found within limitations of the subject. Preliminary
research also helps to refine the topic to be interesting and new. If similar topics are found, then it must be refined by slightly changing the focus. This way the study will bring new knowledge into the discipline. (Green et al., 2006.)

The writing process explained in Picture 14 by Green et al. (2006) is guiding research work under each research paper chapter. The guideline directs best evidence synthesis method to be used in the narrative review. It is explained in detail by Slavin (1995). Slavin (1995) refers it to be the guiding research method when forming a narrative literature research paper. The purpose of the best evidence synthesis is pursuing to be clear on how results are presented and give control to the reader to form decisions based on “where the weight of evidence lies” (Slavin, 1995, p.17). Evidence criteria present how research papers are selected. It must be clear and adequate to understand the selection so clearly; that same resulting papers could be retrieved using the same method. All selections and exclusions should be justified. (Slavin, 1995.)

The writing process described by Green et al. (2006) formulates different chapters starting from title all the way to references. The title should wake interest and explain the topic under review clearly. Abstract summarises the article. It is the most important part of the study in literature research point of view since it is the text that supports reader’s decision whether the whole text is retrieved and incorporated into the study or not. The introduction is explaining research purpose and the point of the research paper. Methods section explains how the study was formed step by step. Search engines and search terms must be listed to explain the scope of the research. From results, there should be listed starting and ending year of searched papers. Search terms and delimiting factors must also be revealed to explain that all relevant research papers were included and sufficiently limited to support the research. (Green et al., 2006.)

In the discussion, the writer must synthesise all information into understandable paragraphs. Order of presented information should follow structure already familiar to the reader. Limitations must also be considered to indicate weaknesses in the paper, and there may be problems with focusing it. In conclusion, the purpose is bound to the study. Findings are listed in clear format, and new things that are found in the study are brought up one more time. All conclusions must be supported by the literature reviewed during the study. The conclusion also reveals ideas and suggestions about future research. Acknowledgements are used if there was someone you want to give credits for. The last part contains references. It should include all references with viable information so that anyone can retrieve original research information used in the study. (Green et al., 2006.)

Narrative overviews, as also literature reviews, merge previous research papers and pull information from different areas into one paper (Baumeister & Leary, 1997; Green et al., 2006; Rowe, 2014). The resulting research paper can provide criticism from each study included and report author’s findings from previous studies. Overview must still be objective and thrive to be truthful to avoid reporting opinions instead of data sourced from the selected research papers. (Green et al., 2006.)
Consolidate previous research
Number of articles must be extensive
Limits are visible in article selection
Focus of the articles are in the past
Content is centered in previous research
Comprehensive bibliographies

| Picture 15 Research Article goals (Schwarz, Mehta, Johnson, & Chin, 2007) |

Picture 15 presents another literature review goals. This another research goal perspective supports Green et al. (2006) goals. This process and goals were defined by Schwarz et al. (2007). As also stated in Green et al. (2006), this method also consolidates previous research to make a new combination of ideas. Similarly to previously presented literature review writing guides, the number of research articles must be extensive to bet wide perspective over the subject, but also limits of the subject should be considered properly so that these boundaries are strictly kept. Focus of the selected articles must be in the past, not studies of the future or suggestions for future research. Using research papers concentrated into the past sets the focus of the papers to be centred in the previous research. To be a broad view of disciplines selected there should be a full suite of bibliographies to support as many perspectives as possible within the limits of the literature review. (Schwarz et al., 2007.)

The narrative literature review should deliver something new to science (Baumeister & Leary, 1997; Rumrill & Fitzgerald, 2001). Therefore, new information and ideas should be harvested from prior research. Integrative theory should already be included in the introduction chapter. It then would give input for making the reading decision on reading the whole study. (Beaumeister & Leary, 1997.)

Chapter 3.1 explained the concepts of literature research and the narrative literature review. Since the idea of the narrative literature review was slightly different on every research paper presented, Chapter 3.2 will explain how the research method was applied in this study.

3.2 Application of research method

In the first phase of this study, research literature was searched in order to compile conceptually difficult areas of inter-organisational trust, trust, ISM and ISMS. This broad research area was then focused on phase 3 to apply rigorously narrative literature review method on inter-organisational trust. Since the purpose of this study was to get elements affecting inter-organisational trust, the most weighting part of literature was retrieved from there. Resulting elements of inter-organisational trust were then categorised using ISMS steps from ISO/IEC 27001 (2013) to help security professionals understand how each element could be mapped to reality. Next is discussed how the process of this study was conducted following the limitations found in the application of narrative literature review.
Picture 16 opens phases how selected research method was applied. The first phase of the study was to source concepts of inter-organizational trust, ISM and ISMS by using Scopus abstract and citation database. The concepts of “inter-organisational trust” and “trust” were covered by utilising search sentences in Scopus using words described in Table 1. Results of this first phase are concluded as the content of Chapter 2.1 and Chapter 2.2 of this study.

Table 1 Tracking of concept searches in Scopus.

<table>
<thead>
<tr>
<th>Search terms</th>
<th>Search field</th>
<th># Hits</th>
<th># Selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;inter-organizational trust&quot;</td>
<td>Article Title</td>
<td>28</td>
<td>2</td>
</tr>
<tr>
<td>“trust”</td>
<td>Article Title</td>
<td>31746</td>
<td>3</td>
</tr>
<tr>
<td>“information security management”</td>
<td>Article Title</td>
<td>243</td>
<td>8</td>
</tr>
<tr>
<td>“information security”</td>
<td>Article Title</td>
<td>2922</td>
<td>15</td>
</tr>
</tbody>
</table>

As described in Table 1 literature search was limited by using search terms listed in “Search terms” column and using the “Search field” to restrict the search into “Article Title” field only. The literature search was conducted 23.10.2016 to Scopus database. Search time was not restricted, and the number of resulting articles is listed in “#Hits” column. Inclusion count of articles into the research material is listed in the last “#Selected” column.

A literature search was conducted with limiting resulting number of articles. The language was chosen to be only English, and only those papers have been selected for which full text was available to be downloaded under license of the University of Oulu or by using Google Scholar and retrieved by public access. All books and retracted papers were also excluded, and only articles, reviews and conference papers were included. Finally, search terms text were used to limit results only to contain papers that
included search terms in the article title of the research paper. Research papers were searched by using Scopus abstract and citation database.

The articles were sorted in Scopus by citing value and those articles which topic indicated support for the topic at hand was taken into the abstract analysis. The final selection was made according to if content relevantly endorsed the concept describing topic currently under processing. These topics are listed in Table 1 in Search Terms column. The resulting research papers selected for this phase are given in Appendix 2.

As displayed in Picture 16 the second phase of this study was to source ISMS building steps from ISO/IEC 27001 (2013) and research literature. These steps were listed in Chapter 2.3, and they were used as a method of categorization of found inter-organisational trust affecting elements in Chapter 4.

The third phase of the study shown in Picture 16, was collecting elements affecting to inter-organisational trust by utilising narrative literature review method. These elements were later on listed and analysed in Chapter 4 as a continuance of the concepts presented in Chapter 2.1 about the inter-organisational trust.

<table>
<thead>
<tr>
<th>Search terms</th>
<th>Search field</th>
<th># Hits</th>
<th># Selected</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;inter-organizational trust&quot;</td>
<td>Article Title</td>
<td>28</td>
<td>19</td>
</tr>
<tr>
<td>&quot;inter-organizational trust&quot;</td>
<td>Article Title</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>AND “security”</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

As described in Table 2 narrative literature review was limited by using search terms listed in “Search terms” column and using the “Search field” to restrict the search into “Article Title” field only. The literature search was conducted 23.10.2016 to Scopus database. Search time was not restricted, and the number of resulting articles is listed in “#Hits” column. Inclusion count of articles into the research material is listed in the last “#Selected” column.

A literature search was conducted with limiting resulting number of articles. The language was chosen to be only English, and only those papers have been selected for which full text was available to be downloaded under license of the University of Oulu or accessed by using Google Scholar for public download. All books and retracted papers were also excluded, and only articles, reviews and conference papers were included. Finally, search terms text were used to limit results only to contain papers that included search terms in the article title of the research paper. Research papers were searched by using Scopus abstract and citation database. From all research papers, the abstract was analysed, and the final selection was made according to if it included inter-organisational trust building elements. The resulting research papers selected are listed in Appendix 1.

The fourth phase of this study was listing elements found in narrative literature review from the viewpoint of trust affecting elements. In this phase, the found elements were
divided into ISO/IEC 27003 (2010) ISMS building steps explained in Chapter 2.3. These trust elements were reported in Chapter 4 as a continuance of trust and ISMS steps.
4. Elements affecting inter-organisational trust

As Savolainen (2008) expresses, there is no generally accepted concept of trust among researchers. This results, that there is no accepted definition of inter-organisational trust. In the inter-organisational level, the trust has broader coverage than in individual level, and it is placed into partnering organisation by trusting organisation. It spreads the assumptions of partner actions between organisations. Inter-organisational trust has direct effects on lowered costs. Inter-organisational trust effects are therefore part of cooperative actions between organisations. (Zaheer et al., 1998.)

In search of effecting factors to inter-organisational trust, this study found several supporting and resisting elements. The elements found from the narrative literature review were divided into categories found in ISO/IEC 27003 (2010) ISMS implementation guidance to concretely support inter-organisational trust building in each implementation step. Each element was firstly listed into groups by similarity, and each group were analysed to belong one of the ISO/IEC 27003 (2010) steps by utilising personal security experience over the subject. This categorization was chosen to support the work of information security professionals by providing guidance what kind of elements are related to which implementation phase. Inter-organisational trust effecting elements are explained, and categorization is linked to ISMS implementation steps by using chapter division.

4.1.1 Obtaining management approval for initiating an ISMS project

Commitment and resources need to be obtained from management as they need to decide resources that are efficiently enabling ISMS implementation work (Beckers, 2014). To support decision-making management require understanding financial implications of ISMS, which are listed in Picture 17.
Monetary elements of trust building are presented in Picture 17. Financial limitations of organisations have positive effect to trust since it directs them to outsource work or use supply chains in business (Seppänen et al., 2007). Uncertainty negates the forces on business, and it affects positively to trust since trust grows at uncertain times (Gaur, Mukherjee, Gaur, & Schmid, 2011; Wei, Wong, & Lai, 2012). Economic hostage-based trust is bound to support costs which arise when the supplier is required to invest before co-operation can start and loss of possibility to choose a cheaper supplier in pursuing on continuity of business co-operation (Dyer & Chu, 2011). Investments in assets required to participate in a partnership are a signal of trust and indicate long-term cooperation (Ashnai, Henneberg, Naudé, & Francescucci, 2016; Liu, 2009). Investment in trust can also be capability development and demand high-quality components from suppliers (MacDuffie, 2011). Cutting supplier costs as bargaining lower prices will affect negatively to inter-organisational trust in the form of cost competitiveness (MacDuffie, 2011). It is good to remind, that trust is also supporting financial performance (Biggiero & Sevi, 2008; Fiala, Prokop, & Živelová, 2012; Gaur et al., 2011; Song & Chen, 2013). According to Biggiero and Sevi (2008), this financial benefit can be achieved example by helping organisations to select best quality suppliers, and Fiala et al. (2012) open up cost savings related to lowered negotiation costs.

Trust governance costs relate to controlling and monitoring opportunism (Gedeon, 2015; Zucker, 1987). According to Zhao (2010), Ratnasingam (2001) and Wei et al. (2012), integrations of IT systems is an investment for building trust. Covering issues over contractually agreed boundaries can be used to enhance inter-organisational trust and reinforce the value of a partner in the trust network (MacDuffie, 2011).

<table>
<thead>
<tr>
<th>Financial incentives</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Financial limitations (Seppänen et al., 2007)</td>
</tr>
<tr>
<td>• Uncertainty (Gaur et al., 2011; Wei et al., 2012)</td>
</tr>
<tr>
<td>• Economic hostage-based trust (Dyer &amp; Chu, 2011)</td>
</tr>
<tr>
<td>• Cost competitiveness (MacDuffie, 2011)</td>
</tr>
<tr>
<td>• Trust support performance ((Biggiero &amp; Sevi, 2008; Fiala, Prokop, &amp; Živelová, 2012; Gaur et al., 2011; Song &amp; Chen, 2013)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Investments to co-operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Supporting costs (Dyer &amp; Chu, 2011)</td>
</tr>
<tr>
<td>• Loss of low-cost suppliers, opportunity-cost (Dyer &amp; Chu, 2011)</td>
</tr>
<tr>
<td>• Integration of systems (Zhao, 2010; Ratnasingam, 2001; Wei et al., 2012)</td>
</tr>
<tr>
<td>• Extra-contractual actions (MacDuffie, 2011)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trust governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Contracts, agreements (Gedeon, 2015; Ratnasingam, 2001; Gaur et al., 2011)</td>
</tr>
<tr>
<td>• Monitoring costs (Gedeon, 2015; Zucker, 1987)</td>
</tr>
<tr>
<td>• Countries economic elements (Dyer &amp; Chu, 2011)</td>
</tr>
</tbody>
</table>
Gedeon (2015), Ratnasingam (2001) and Gaur et al. (2011) listed controlling elements increasing costs such as contracts and agreements. Zhang (2011) and Gaur et al. (2011) also pointed, that contracts cannot be written to comprehend every situation to control all risks involved. Therefore trust is a necessary extension of it. Governance costs can be substituted to lower overall costs and performance can be improved by enhancing inter-organisational trust (Zhao et al., 2010). Costs related to controlling abuse and abusing opportunism despite the control elements affect costs on both sides of partnership (Barney & Hansen, 1994).

Economic factors in trust building are possibly increasing costs, and they should be analysed that they fit into business and eventually return the investment (Dyer & Chu, 2011). Hexmoor et al. (2006) explained trust being path-defined property; it should be considered when resourcing trust controls. Path-defined property indicates, that it is constructed gradually, but destroyed instantly by one event (Hexmoor et al., 2006). Finally, economic elements of countries are also considered supporting trust (Dyer & Chu, 2011).

![Picture 18](Cultural elements related to inter-organisational trust.)

**Picture 18** lists cultural elements of trust. Shared values lower barriers to enable trust (Seppänen et al., 2007). Culture, as it is surrounding individuals in organisations, have the effect to trust through values, rewards and beliefs (Zucker, 1987). The social similarity in ethical identity ease is building trust (Zucker, 1987). Castelfranchi (2008) draws trust as human feeling in mental attitude, willingness and belief soaked from culture. Mutual beliefs also help build trust (Castelfranchi, 2008; Hexmoor et al., 2006; Zucker, 1987). Hexmoor et al. (2006) explained trust as being able to predict others behaviour to be something as expected.

Countries also direct organisations with the help of institutional mechanics to use trustworthy standards, that support trust building work (Zucker, 1987). Institutions such as banks or organisations organising labour have institutional-trust injected into their society-level tasks (Zucker, 1987). Coordination of cyber security defences, country
level guidance and related operations to support security goals in national level effects institutional level of trust (Murdoch & Leaver, 2015). Vélez et al. (2008) also introduced personnel-cultural controls in the form of satisfaction surveys, meetings and training planning to support trust building. Also similar cultural and national background supports trust (Noordin, Bititci, & Van Der Meer, 2012).

In individual level elements affecting trust are quantified as “feeling of being competent, a feeling of safety and caring, a sense of autonomy and empowerment, consistency and fairness in social relationships, congruence in the values of an individual and the organization” (Savolainen, 2008, p.6). Control and trust must also be balanced by management to support organisational culture (Savolainen, 2008). Confidence towards partners and its opposing force suspicion also have the effect of trusting balance in individual level (Vélez et al., 2008).

**Picture 19** Asset sharing elements supporting inter-organisational trust.

**Picture 19** presents elements affecting trust in asset sharing. Assets being those items that are protected by risk management, they are vital elements to business (Blakley et al., 2001). According to Hexmoor et al. (2006) sharing this kind of essential aspects of business increase trustworthiness. Marketing information shared between supply chain participants influence positively to trust (Vélez et al., 2008).

One of the assets in modern business is knowledge assets, sharing this information also have a positive effect to trustworthiness (Ashnai et al., 2016; Gaur et al., 2011; Hexmoor et al., 2006; Noordin et al., 2012; Wei et al., 2012). On the other hand, sharing critical asset information and especially tacit knowledge requires also trust to succeed (Savolainen, 2008; Vélez et al., 2008; Zhao et al., 2010). More generally expressed, trust is supporting open communication and vice versa (Ratnasingam, 2001; Savolainen, 2008).
Trust elements from status and identity is presented in **Picture 20**. Who and what partner is affects also to trust (Barney & Hansen, 1994). Business success is affecting the status of the partner and also building trust (Vélez et al., 2008). Mutual organisation size and dependency support inter-organisational trust and balance in powers (Hagedoorn, Roijakkers, & Van Kranenburg, 2008).

In systems designed to distribute confidential information such as incident reporting systems, anonymity together with trust also supports information sharing (Murdoch & Leaver, 2015). Therefore, information is shared in its social context, where trust building can be backed up by utilising social networking features (Murdoch & Leaver, 2015). This information sharing is related to security incident reporting in country level. Such a system in the United Kingdom is designed to follow social media methods in a way that authors can deliver basic professional profile, contact others in the trust network, control how their inputted information can be shared, and also ability choosing information sharing to be anonymous (Murdoch & Leaver, 2015). The system enables collection of general incident information so that every stakeholder can learn about new threats, attacks and mitigation steps taken. This finding is partially conflicting in findings on identification found to be supporting trust building (de Oliveira Albuquerque et al., 2014; Hexmoor et al., 2006).

Similarities in language, location and mutual trust also support trust building in knowledge sharing perspective (Savolainen, 2008). The professional and correct language used by professionals are a proof of competence, and it builds trust (Gedeon, 2015; Noordin et al., 2012). Intent to establish trust relationship in management actions, security policies, mission statements and actual behaviour based on reciprocity are supporting trust building (Gedeon, 2015). Manager direction in the case to fix issues negatively affecting trust is regarded also supporting trust building, and this effect is
enhanced by utilising feedback mechanisms on trust supporting actions (Gedeon, 2015). In behaviour, experienced rationality is also supporting trust (Ratnasingam, 2001).

### 4.1.2 Defining ISMS scope, boundaries and ISMS policy

**Picture 21** Elements affecting inter-organisational trust in information handling.

**Picture 21** Elements affecting inter-organisational trust in interaction.

Information handling guidelines

- Sensitive information handling (Murdoch & Leaver, 2015)
- Technology (Murdoch & Leaver, 2015)
- Processes (Murdoch & Leaver, 2015; MacDuffie, 2011)

Culture

- See Picture 18.

Leadership

- Social information sharing system (Savolainen, 2008)

**Picture 22** Elements affecting inter-organisational trust in interaction.

Communication

- Nature (Seppänen et al., 2007)
- Quality (Järveläinen, 2012; Ratnasingam, 2001; Savolainen, 2008)
- Frequency (Gaur et al., 2011; Järveläinen, 2012; Ratnasingam, 2001; Savolainen, 2008)
- Secure methods (Järveläinen, 2012)
- Privacy (Ratnasingam, 2001)
- Confidentiality (Ratnasingam, 2001)

Reliability

- Interaction and service reliability (Järveläinen, 2012; Seppänen et al., 2007)
- Assigning tasks (Vélez et al., 2008)

Support

- Achieve compliance (Dyer & Chu, 2011; Savolainen, 2008)
- Providing assistance (Zhang, 2011)
- Problem solving capability (Vélez et al., 2008)
Interaction related elements affecting trust are presented in Picture 22. Trust per se is generating interaction and social relationships between organisations (Savolainen, 2008). Good quality communication need to be emphasised (Järveläinen, 2012; Ratnasingam, 2001; Savolainen, 2008). The way communication is handled effects of trusting building (Seppänen et al., 2007). Communication needs to be suitable for frequency (Gaur et al., 2011; Järveläinen, 2012; Ratnasingam, 2001; Savolainen, 2008). Sensitive information must be communicated secure way (Järveläinen, 2012). As Ratnasingam (2001) explains privacy and confidentiality need to be also taken care to support trust building.

Interaction and service reliability also supports positively trust (Järveläinen, 2012; Seppänen et al., 2007). When tasks are assigned over organisational boundaries, it also builds trust (Vélez et al., 2008). Binding resources to supporting and assisting partners on tasks related to services provided or supporting compliance work also benefit trust building (Dyer & Chu, 2011; Savolainen, 2008). Providing assistance to partner is also supporting trust building (Zhang, 2011). Problem-solving capabilities of a partner support trust (Vélez et al., 2008; Zhang, 2011). It is also good to notice that binding resources for support work increase trust costs (Dyer & Chu, 2011; Zucker, 1987).
Picture 23 reveals elements of the relationship that have powers over the trust. The essence of relationship quality and performance is trust in a way that it creates better quality and performing relationships (Seppänen et al., 2007). Vélez et al. (2008) pointed out also that sacrifices partnering organisation make will also have an effect on trust through relationships quality. One kind of a quality measure is also transparency, which also has a positive effect on trust (Noordin et al., 2012). Trust in relationships is also built by keeping deals and promises (Dyer & Chu, 2011; Savolainen, 2008). Positive expectations are components of trust building (Hexmoor et al., 2006; Savolainen, 2008; Vélez et al., 2008; Zaheer et al., 1998). Reciprocity is supporting trust building (Castelfranchi, 2008; Hexmoor et al., 2006). On the other hand, willingness to reciprocate is not automatically resulting trusting someone (Castelfranchi, 2008). Fairness and credibility also quantify trust building (Savolainen, 2008; Seppänen et al., 2007). Dependency between business partners has an adverse effect on trust (Gaur et al., 2011; Vélez et al., 2008; Young-Ybarra & Wiersema, 1999).

Relationships are linking back to interaction quality; that was listed in Picture 22. When starting business co-operation, trust is stronger and bound to social ties in individual-
level, and later on, trust is begun to scatter around business processes all around the organisations to vanish from individual-level (Seppänen et al., 2007; Zhang, 2011). The length of the partnership is also affecting positively to trust (Gaur et al., 2011; Ratnasingam, 2001). Relationship lengths build trust into individual-level between organisational members when personnel are staying at the same position for a long time (Dyer & Chu, 2011; Gaur et al., 2011). Consistency builds trust (Ratnasingam, 2001). Past experience also influences to trust experience (Biggiero & Sevi, 2008; Noordin et al., 2012; Ratnasingam, 2001). Face to face working methods support also trust building because it is easier to analyse the behaviour of other and build social ties (Dyer & Chu, 2011). When organisations and interacting individuals or groups are in close proximity, it increases number face to face meetings and therefore supports trust building (Dyer & Chu, 2011). Relationships bring people back to the centre of trust and information security (de Oliveira Albuquerque et al., 2014).

Stability in employment also makes social connections between executives stronger (Dyer & Chu, 2011). In case personnel changes are constant, changes can be seen in management, staff and policies; then trust building can be directed to processes and routines as institutionalised behaviour to support inter-organisational trust growth (Dyer & Chu, 2011). Personal level relationships develop through time, so changes in the organisation have a negative effect on inter-organisational trust bound to individuals (Dyer & Chu, 2011).

When measuring relationship, length and depth of it is affecting to relationship-based trust especially individual-level when personal contacts are built (Dyer & Chu, 2011). Relationship-based trust is based on social motives such as depth and sanctions (Dyer & Chu, 2011). Hexmoor et al. (2006) introduced more motives, such as control and influence. Together these act as controls in relationship-based trust (Dyer & Chu, 2011). Individual-level sanctions in social sanctions are “risk of losing love, respect, prestige and/or (worst of all) banishment from the social community” (Dyer & Chu, 2011, p.12). Social control in trust can be strong when there is a risk of losing it (Dyer & Chu, 2011; Liu, 2009). Through personal level relationships inter-organisational trust is also enhanced (Zaheer et al., 1998).

4.1.3 Conducting information security requirements analysis

Opportunism

- Rewards (Barney & Hansen, 1994)
- Exploit visible (Dyer & Chu, 2011)
- Exploit costs (Dyer & Chu, 2011)
- Profits (Liu, 2009)
- Balance of trust and control (Savolainen, 2008)

Picture 24 Inter-organisational trust elements of opportunism control.

Opportunism control related trust elements are shown in Picture 24. Opportunism requires control, and it binds resources (Zaheer et al., 1998; Zucker, 1987). Barney and Hansen (1994) proposes rewards embedded into control systems to enhance trust building, but increase costs even more. When business co-operation requires bringing forward opportunities for exploitation, then trust should be controlled in a way that it would bring up high costs to exploiter (Dyer & Chu, 2011). Lowering possibilities to profit from exploiting opportunism builds trust (Liu, 2009). A Higher level of trust has cost-lowering effect in inter-organisational trust, and only sufficient controls should be
implemented in protecting opportunism (Hexmoor et al., 2006). Controls also build trust (Järveläinen, 2012). When control is reduced, and power is provided, then trust is needed (Gaur et al., 2011; Mayer et al., 1995). Management must evaluate the balance between control and trust to suit organisational culture (Savolainen, 2008).

4.1.4 Conducting risk assessment and planning risk treatment

| Control mechanism | • Audits (Järveläinen, 2012)  
|                   | • Power transfers (Järveläinen, 2012)  
|                   | • Measurements (Gedeon, 2015)  
|                   | • Governance tools implementation (Järveläinen, 2012)  
|                   | • Third party evaluations (Zucker, 1987)  
|                   | • Standards  
|                   | • Contractual binding  
| Reputation | • Training business partners (Järveläinen, 2012)  
|           | • Good reputation (Zhang, 2011; Biggiero & Sevi, 2008)  
|           | • Recommendations and past actions (Hexmoor et al., 2006; MacDuffie, 2011)  

**Picture 25** Inter-organisational trust elements in audits and assessments.

Trust elements of audits and assessments are listed in **Picture 25**. An audit is one control mechanism that supports validation of trustworthiness, and it is related to power transfers, increase power over suppliers and confirmation of security controls implemented into systems (Järveläinen, 2012). In case organisation values trust-building efforts, then trust should be measured to support it grow (Gedeon, 2015). Using governance tools, such as ISO/IEC 27001 (2013), business partners are evaluated to be trustworthy (Järveläinen, 2012). By using third party evaluations and audits inter-organisational trust can be improved (Zucker, 1987).

Enhancements to trust can also be achieved conducting inter-organisational training for business partners like security training and therefore incurring the burden of knowledge sharing tasks, support continuity and helping suppliers (Järveläinen, 2012). This also effects to reputation among social and business contacts and it is supporting trust building (Järveläinen, 2012). A good reputation is supporting trust (Biggiero & Sevi, 2008; Zhang, 2011). Recommendations of other trusted organisational members and past actions example related to losing trust have also profound effect (Hexmoor et al., 2006; MacDuffie, 2011).
Legal and contractual elements supporting inter-organisational trust.

Järveläinen (2012) noted that even characteristics of SLA contracts could have the effect on trust building. Also conducting security clearances, granting access to only those systems that are needed, and non-disclosure agreements (NDA) together with demanding signatures to binding security policies can support trust (Järveläinen, 2012). Contractual arrangements and governance increase costs and protection (Barney & Hansen, 1994). Higher sub-contractor and supplier control build trust (Järveläinen, 2012).

4.1.5 Designing the ISMS

Picture 26 Legal and contractual elements supporting inter-organisational trust.

Picture 26 lists elements supporting trust in legal and contractual perspective. Legal and contractual elements are used to control opportunism by protecting assets (Barney & Hansen, 1994; Järveläinen, 2012). One opposing option to trust is establishing collaboration without trust (MacDuffie, 2011).

Picture 27 Elements of stability that supports inter-organisational trust building.

Picture 27 lists elements of stability that support trust building. Stability can be seen in repeated transactions and formal structures that are visible outside of the organisation (Zucker, 1987). Also, Dyer and Chu (2011) defined process-based trust, that implies institutionalisation in processes and routines of an organisation. Routines as repeatable tasks support trust building (Vélez et al., 2008; Zhang, 2011). Stability in personnel also supports trustworthiness as it can also be seen as commitment (Dyer & Chu, 2011). Commitment to the business relationship has a central role in trust-building (Ashnai et al., 2016; Noordin et al., 2012). Continuity at the expense of loss of low-cost supplier options is a powerful signal of trust, and it can also be seen on employment stability (Dyer & Chu, 2011). Organisational and institutional factors in business stability
enhance trust (Hexmoor et al., 2006). Business continuity management process implemented properly also supports trust in the sense of continuity and stability from partnering perspective (Järveläinen, 2012). Also, stability in personnel limits changes in processes and social ties of executives can grow stronger (Dyer & Chu, 2011).

Chapters 2.1 through 2.2 of this study provided phase one literature research of this study to explain concepts around inter-organisational trust and ISMS implementation. Chapter 2.3 continued to extract implementation steps required to establish an ISMS and finally, Chapter 4 listed trust effecting elements categorised under ISO/IEC 27001 (2013) implementation steps. This Chapter 4 provides results of narrative literature review and this study. Trust effecting elements were presented first in pictures, as a list of items and then each was explained by the literature.

As it was seen in this Chapter 4, there are many inter-organisational trust elements. It is required to create auditable evidence so that it would be easier to distinguish organisation’s trustworthiness instead of only claiming to be one (Barney & Hansen, 1994). Next chapters open discussion and implications.
5. Discussion and implications

The current study analysed supporting and resisting elements of inter-organisational trust. This study did not find exactly matching papers from the research literature to cover inter-organisational trust building in ISMS implementation. The study was motivated by this finding, which was found already in preliminary literature research phase. Due to this research gap, several topics for future research were listed.

The research question of this study was “How to support inter-organisational trust by ISMS implementation?”. Implementing ISMS was the central part of this study as a categorization method. Inter-organisational trust building elements were retrieved from the literature by using narrative literature review. These elements were positioned into the ISMS implementation phases described in ISO/IEC 27001 (2013). This categorization of effecting elements raised trust support in a format that can be easily applied by all information security professionals.

Picture 28 Results of the study.
The resulting analysis of inter-organisational trust affecting elements is presented in Picture 28. Results are categorised into ISMS implementation steps found from ISO/IEC 27001 (2013). Picture concludes the results of this study as the study method was narrative literature review the only new information is the categorization and gathering of inter-organisational trust elements into one study. To understand the phenomenon of inter-organizational trust in the context of ISMS implementation and to create a consistent basis for improving an organisation’s ISM approaches from the perspective of trust building, individual trust elements were incorporated into a holistic framework (see Picture 28). A framework thus offers a categorization that reduces a broad range of concepts to a more manageable framework for both security practitioners and researchers.

![Graph of inter-organisational trust effecting elements](image)

**Picture 29** Inter-organisational trust effecting elements found in the study.

Distribution of inter-organisational trust effecting elements found in this study can be seen in **Picture 29**. This study found 102 different elements that can affect to inter-organisational trust. The largest number of elements was found from inter-organisational relationships.

This study combined ISMS and inter-organisational trust elements and categorised them into ISO/IEC 27001 (2013) implementation steps to achieve fluent applicability and understanding among information security professionals. This approach seemed to be new among research papers regarding inter-organisational trust. It was very rare that research papers were able to raise their findings into such a concrete level as this study did. This was another motivation to gather the results under understandable format, that could be used easily by an information security professional.

By reading this study a manager can adjust thoughts on benefits ISMS and trust-building bring and also understand their linking to ISMS implementation. Security specialists also can get viewpoint towards management, since elements of trust familiarised in this study are affecting managerial decisions example on outsourcing, contracting, business relationships and usage of supply chains. Therefore, enabling managers and security specialists to understand each other’s work can be listed as one implication of this study.
6. Conclusions

The aim of the review was to identify supporting and resisting elements of inter-organisational trust when implementing ISMS. The study resulted in the list of inter-organisational elements categorised into ISO/IEC 27001 (2013) ISMS implementation steps. Using common ISMS implementation steps brought complex phenomenon of inter-organisational trust in the hands of security professionals. The study was also bringing management and security specialist closer together in terms of vocabulary and context understanding.

ISMS-related inter-organisational trust was not researched properly. This was noted already at preliminary literature research. Since ISMS and inter-organisational trust consists of at least 3 different disciplines of administrative, behavioural and informational sciences it seems to be a combination of which is not researched together properly. One of the main findings was the research gap found there.

This study started filling this research gap between trust and implementation of ISMS. This study extracted elements that can help building inter-organisational trust and categorising them into ISO/IEC 27003 (2010) ISMS implementation steps to help information security specialists and managers to understand how the implementation of ISMS can have the effect to trust. This study also revealed that ISMS and trust should be studied together, but since they are presented in different disciplines as in administrative, behaviour and information science it is rarely available in any single school’s curriculum.

The study limited the research into a very narrow area between information processing science, behaviour sciences and discipline of management. As information security is multidisciplinary phenomenon, knowledge from all of these areas are required to be a successful implementer of information security in corporate level (Porvari, 2012).

Inter-organisational trust building in this study was limited to analysing effecting elements only from implementation perspective of ISMS and inter-organisational trust. The phenomenon of trust is investigated only between companies, not between institutions, organisations and customers, or people inside an organisation or a group.

A narrative literature review was used as an information source to point out research gap found already during preliminary literature review. The gap was discovered on the research topic formed in conjunction of inter-organisational trust and ISMS. Due to this gap, there were no exactly relevant research papers found from the research literature, therefore, the findings of this study, the elements are retrieved from surrounding literature and present one limitation in this research.

Selection of articles included in narrative literature review about inter-organisational trust was limited to those that considered an inter-organisational trust. All research papers needed to be able to be retrieved with full-text by either using license of the University of Oulu in Scopus search engine or by utilising Google scholar to retrieve publicly available versions. No books were included in the study. Only articles, reviews and conference papers were included. Research papers in languages of English were
accepted. Those papers with an indication of retraction and articles not containing any trust supporting elements were also excluded from the study.

Another limitation of this study was applied research method in phase 1. The applied narrative literature review could have been accomplished with strict search words and research paper selection. Due to lack of proper rigorous attitude the concepts defined in Chapter 2.1 and 2.2 were not following selected method properly as described in Chapter 3.1. That is why concept finding part is called as literature search.

A narrative literature review was applied rigorously in phase 3, where inter-organisational trust was researched. Limitations were used in using just one linguistic form as “inter-organizational trust”. This resulted in enough research papers for the study, but it could have been a larger sample with using several word combinations such as: “inter-organisational trust”, “intra trust”, “interorganizational trust”, “inter organisational” or “interorganizational trust”, which all were found from the research papers found.

Trust concept varies from the level it is observed (Rousseau et al., 1998). There is no generally accepted concept of trust among researchers (Savolainen, 2008). This indicates the core problems in trust research. On top of that, there is only a few or none ISMS research related to inter-organisational trust. This study found none.

Many researchers have stated that business requires trust (Castelfranchi, 2008; de Oliveira Albuquerque et al., 2014; Dyer & Chu, 2011; Seppänen et al., 2007). Implementing ISMS is one way to build trust (ISO/IEC 27003, 2010). These topics of trust and ISMS implementation should be investigated together through conducting empirical studies. Future empirical studies can apply the framework of inter-organisational trust formulated in this study for building their research instruments (e.g., interviews, questionnaires) and testable hypotheses.

Since the topic of inter-organisational trust and ISMS joins several scientific disciplines together, it should be researched from a multidisciplinary perspective to determine if the combination of different disciplines related to the problem scene is affecting negatively to research interest. Complicacy of the research subject and a requirement to understand the vast amount of various disciplines is not directly supporting any individually, but together supporting the research topic. Business and information security should be taught together to support this finding.

Effects of trust are not thoroughly researched in the scope of ISMS implementation. Investment into ISMS in business can be justified in many ways, but usually, it is not aligned to trust building. Information security professionals can use this research paper justifying the investments to the management. Trust is eventually the driving force before companies exchange confidential or critical business information. Actually, it is one of the main driving forces of any business.
Picture 30 sourced from Scopus search results explains the division of research subject areas in conjunction with trust and information security. This result was received using search words “trust” and “information security”, using Article Title, Abstract and, Keywords as search fields. Scopus resulted in total 601 papers, and 43 are from Business perspective. By using search word “trust” only, it resulted in 123 629 research papers. By continuing the search and changing search words to “inter-organizational trust” and “ISMS” or “information security management system” result is 0. This opens the research gap discovered by this study.

Inter-connection of inter-organisational trust and business reveals several new research topics. Investments into inter-organisational trust-building and how it benefits business co-operation should be researched. Also, monetary benefits gaining inter-organisational trust and cost of losing it is not properly researched. Interesting viewpoint of return on investment (ROI) in inter-organisational trust and then losing the investment cost is not researched at all or researched very limitedly.

Another research direction would be studying costs of inter-organisational trust as Dyer and Chu (2011) proposed. This building cost perspective combined with costs related to losing trust would be fascinating. Of course when costs are considered, then also return would be interesting to keep in the equation. Benefits of having trust in co-operation should be researched together with costs to reveal elements impact to business properly.

The combination of managerial studies and information security in inter-organisational trust scope is researched very superficially. Management discipline should be researching ISM and vice versa. Information security should be seen as one of the most important management systems supporting business operations and keeping business functioning as expected. The gap is easily spotted due to that interests of the research of these two disciplines have followed such different paths. This indicates that there should be education paths for students where both disciplines would be introduced.
References


Beckers, K. (2014). *Goal-based establishment of an information security management system compliant to ISO 27001*


Zhao, F., Ling, H., & Xu, Z. (2010). Inter-organizational trust and supply chain flexibility: From a relational view of the firm. 2010 International Conference for Internet Technology and Secured Transactions, ICITST 2010,

Appendix 1 References for inter-organisational trust


Appendix 2 References for describing key concepts


Beckers, K. (2014). *Goal-based establishment of an information security management system compliant to ISO 27001*


