Anniina Ojalainen

ISO 27001 INFORMATION SECURITY MANAGEMENT STANDARD'S IMPLEMENTATION IN SOFTWARE DEVELOPMENT ENVIRONMENT: A CASE STUDY

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2020

ABSTRACT

Ojalainen, Anniina
ISO 27001 Information Security Management Standard's Implementation in Software Development Environment: A Case Study
Jyväskylä: University of Jyväskylä, 2020, 86 pp.
Cyber Security, Master's Thesis
Supervisor(s): Soliman, Wael

ISO 27001 information security management standard provides guidelines to organizations to evaluate and document their information security processes. However, information security management standards have been criticized to focus on the existence of the process but not its actual content. This Master's Thesis aims to assess ISO 27001's suitability to software development environment and its impact on employees' practices and experiences in secure software development. This thesis observed these phenomena through the following research questions: "How employees experience the ISO 27001 standard's implementation in a software development environment?", "What kind of conflicts might appear between ISO 27001 standard requirements and day-to-day work?" and "How the target unit resolves the conflicts between ISO 27001 standard requirements and day-to-day work?". This thesis consists of a literature review and an empirical research which was conducted as a qualitative case study. The study's data was collected by conducting semi-structured interviews in an organization operating in ICT. The target organization had acquired a software development company which was merged to the organization as a software development unit. The research questions were observed in the software development unit through a contextualisation framework and research themes that revolved around changes in target unit's information security culture and practices, process of ISO 27001 implementation and employees' experiences of the process and changes. The results of the study propose that ISO 27001 can influence employees' attitudes and compliance towards information security policies. On the other hand, ISO 27001 causes conflicts between its requirements and organization's practical demands. In this study, the conflicts were related to code reviewing and disciplinary measures documentation. The code reviewing process was resolved based on known vulnerability assessment mechanisms. Conflicts related to disciplinary measures were not fully resolved: the target organization had to answer to the unsuitable standard requirements but after the auditing the disciplinary measures got relegated to the background. The findings of the study indicate that as in projects, in information security management standard implementation employees' involvement, management's support and sufficient communication are crucial to make the employees' experiences more positive.

Keywords: information security, standard, ISO 27001, standard implementation

TIIVISTELMÄ

Ojalainen, Anniina
Tapaustutkimus ISO 27001 tietoturvastandardin implementaatiosta ohjelmistokehitysympäristössä
Jyväskylä: Jyväskylän yliopisto, 2020, 86 s.
Kyberturvallisuus, Pro Gradu -tutkielma
Ohjaaja(t): Soliman, Wael

ISO 27001 -tietoturvastandardi ohjaa organisaatiot arvioimaan ja dokumentoimaan tietoturvaprosessejaan. Tietoturvastandardeja on kritisoitu pelkkien prosessien olemassaoloon keskittymiseen prosessien sisällöllisten seikkojen kustannuksella. Tämän Pro Gradu -tutkielman tarkoituksena on arvioida ISO 27001: n soveltuvuutta ohjelmistokehitysympäristöön ja sen vaikutusta työntekijöiden käyttäytymiseen ja kokemuksiin turvallisesta ohjelmistokehityksestä. Tutkielmassa havainnoitiin näitä ilmiöitä seuraavien tutkimuskysymysten avulla: "*Kuinka työntekijät kokevat ISO 27001 -standardin käyttöönoton ohjelmistokehitysympäristössä?*", "*Millaisia ristiriitoja saattaa ilmetä ISO / IEC 27001 -standardivaatimusten ja päivittäisen työn välillä?*" ja "*Kuinka kohdeyksikkö käsittelee ISO / IEC 27001 -standardin vaatimusten ja päivittäisen työn välisiä ristiriitoja?*". Tämä tutkielma koostettiin kirjallisuuskatsauksesta ja empiirisestä tutkimuksesta, joka toteutettiin laadullisena tapaustutkimuksena. Tutkimuksen data kerättiin tekemällä semistrukturoituja haastatteluja ICT-alalla toimivassa organisaatiossa. Kohdeorganisaatio oli ostanut ohjelmistokehitysyrityksen, joka oston jälkeen sulautettiin organisaatioon ohjelmistokehitysyksiköksi. Tutkimuskysymyksiä havainnoitiin ohjelmistokehitysyksikössä kontekstualisointiviitekehyksen ja eri haastatteluteemojen kautta. Teemat käsittelivät kohdeyksikön tietoturvakulttuurin ja käytäntöjen muutosta, ISO 27001:n jalkauttamisprosessia ja työntekijöiden kokemuksia prosessista ja muutoksista. Tutkimuksen tulokset osoittavat, että ISO 27001 voi vaikuttaa työntekijöiden asenteisiin ja tietoturvakäytänteiden noudattamiseen. Toisaalta ISO 27001 aiheuttaa ristiriitoja standardin vaatimusten ja organisaation käytännön vaatimusten välillä. Ristiriidat liittyivät erityisesti koodikatselmoinnin ja kurinpitotoimien dokumentoitiin. Koodikatselmoinnin haasteet ratkaistiin tunnettujen haavoittuvuuksien arviointimekanismeihin nojaten. Kurinpitotoimiin liittyvää ristiriitaa ei saatu täysin ratkaistua: organisaation oli vastattava standardin osittain soveltumattomiin vaatimuksiin, mutta auditoinnin jälkeen kurinpitotoimenpiteet ja niistä kommunikointi ovat jääneet taka-alalle. Tutkimuksen tulokset osoittavat, että kuten projekteissa, myös tietoturvastandardin jalkauttamisessa työntekijöiden osallistuminen, johdon tuki ja riittävä viestintä ovat ratkaisevan tärkeitä työntekijöiden positiivisten kokemusten lisäämiseksi.

Avainsanat: Tietoturva, standardi, ISO 27001, standardin jalkauttaminen

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

Organizations are relying on information systems increasingly. Information systems are exposed to variety of threats regularly which can compromise the three aspects of information security: confidentiality, integrity, and availability of information. Employees from junior to senior management have responsibility for organization's information security. (Solms & Solms, 2009). Organizations may place information security policies to ensure the quality of information and employees' compliance to secure practices. However, according to Siponen and Vance (2010) even information security policies are implemented and compliance by employees required, many employees do not comply with the policies.

In addition to information security policies, organizations can pursue information security management standard certificates. Information security management standards are one of the most widely used security management methods (Siponen, 2006). Information security certificates can act as an evidence to stakeholders that the organization is executing information security practices. However, based on Vroom's and Solms' (2004) review very little evidence could be found that auditing of the behaviour of the employee regarding information security occurs in practice. There is no guarantee that information security management standards impact employees' information security policy compliance.

Other limitation related to information security management standard, is that standards focus on ensuring that required information security processes and practices exists, while they do not focus on processes' content and how these security processes can be accomplished in practice. Paying attention only to the existence of the process and not the content of it may promote a false sense of security. (Siponen, 2006).

Siponen (2006) proposes that researchers should avoid listing obvious aspects, such as security policy existence or user compliance. Instead, practitioners could benefit from research that focus on in-depth experiences and lessons learned from the organizations that have used and applied information security management standard. Siponen (2006) proposes case or action research which could clarify how security standard objectives are attempted to meet in organizations where information security management standards are applied. Therefore, it is important to study how security standard are implemented in practice and how employees' behavioural changes related to compliance can be observed. In this paper, an ISO 27001 information security management standard implementation process if observed from employees' perspective to better understand the complex nature of security standard application. With these findings, organizations can handle conflicts that may arise during the implementation process with more ease. Thus, the research questions for this study are: *"How employees experience the ISO 27001 standard's implementation in a software development environment?", "What kind of conflicts might appear between ISO / IEC 27001 standard requirements and day-to-day work?"* and *"How the target unit resolves the conflicts between ISO / IEC 27001 standard requirements and day-to-day work?.*

These research questions are studied by conducting a literature review and an empirical research. The literature review aims to map the existing literature related to information security in organizations and factors that affect employees' information security compliance. The literature was gathered by using search tool Google Scholar and some of the well-known publication sites such as MIS Quarterly. To find relevant articles and studies, the following search words and word combinations were used: information security, standard, implementation, management, security behaviour, information security policy compliance. As the results extended to industrial system studies, some limitations were made to focus only on organization's using information systems.

The empirical study was conducted as a qualitative longitudinal single case study. The data for this research was gathered by conducting semi-structured interviews in two different interview rounds with the same employees. The timespan between the interviews were three months. The data was gathered from Finnish organization operating in ICT. The target organization had acquired a software development company and merged it to their organization as a software development unit. The target organization had ISO 27001 certification already, but the new target unit had not been ISO 27001 certified before. Ten employees of the target unit were interviewed. The interviews were transcribed word-to-word and coded based on the interview themes. The themes were the context of the changes that were happening, the conflicts and resolutions related to implementation process and the employees' experiences of the standard implementation and its suitability. In addition, the interviews were analysed through contextual framework.

The reviewed literature did not handle the complexity of the information security management standard implementation. The whole phenomenon could not be handled through individual theories that leave out all the contextual issues. Based on these reviewed theories it was not known how information security management standards affect employees' daily compliance and what kind of conflicts might appear between the standard requirements and employees' daily work requirements. This study tried to capture the implementation process in-depth from employees' viewpoint.

Related to the first research question, the employees' experiences indicated that even ISO 27001 standard claims to be designed in a way where it is flexible enough to be used by every type of an organization, ISO 27001 is not written from the software development perspective and the standard is not suitable for software development environment without contextualized interpretations. ISO 27001 implementation may take a lot of resources and burden the employees working with it. In addition, the employees would have hoped for better communication and guidance from the management. In the end, the target unit passed the standard auditing and notified that ISO 27001 can be interpreted in various ways to pass the auditing.

Regarding the second question, the findings of the study suggest that the conflicts that appeared between the standard requirements and daily work were related to the duality of the ISO 27001 standard: The standard required disciplinary processes to be documented and communicated which did not suit the organization's culture. On the other hand, the target unit studied the standard to find help in finding best practices for code reviewing, but the standard failed to offer any assistance in this.

Regarding the third research question about the resolutions related to the conflicts, it was observed that the target unit reached towards well-known vulnerability documentations to solve the issues related to code reviewing. The disciplinary processes were not handled by the target unit since during the study it was realized that the disciplinary process documentation was not a responsibility of the target unit. However, the interviewees were not familiar with the disciplinary processes at all. Hence it seems that the target organization's resolution was that it does not emphasize ISO 27001 requirements that do not fit into their organizational culture.

This thesis consists of the introduction chapter and six main chapters. The thesis is structured from the main concepts, to literature review, empirical research and then results. In the second chapter, the main concepts of this study are defined, including information security, security threats, insider threats and information security management standards. In the third chapter, the core research themes, and most applied information security compliance theories are introduced. In addition, the theoretical framework for this study is introduced. The fourth chapter describes the research method, data acquisition and research conduction. In the fifth chapter the results of this study are presented. The sixth chapter discusses the findings and limitations of this study, and suggestions for further study. The final chapter concludes the study.

2 KEY INFORMATION SECURITY CONCEPTS

Information technology is gaining an increasingly important role in many organization's business operations and it is included in almost every field of business. Information security is not just a domestic issue: in the electronic commerce world, companies affect their business partners information security through their own security (Solms, 1999). Information security has taken a shift from IT security's technical aspect to managing people, processes, information as well as IT (Humphreys, 2008). Different kinds of technologies, skills and complex solutions are needed to maintain information security. Still, human is the weakest link in information security (Gratian, Bandi, Cukier, Dykstra & Ginther, 2018) but after all organizations must be able to rely on their employees.

In this chapter relevant definitions and concepts are introduced in the context of information security. In chapter 2.1 information security is defined in general. Information security threat classifications are presented in a context of this study in chapter 2.2. The concept of insider threats is introduced in chapter 2.3. Chapter 2.4 focuses on information security management standards and one of the most widely used information security management standard ISO 27001 is introduced. This chapter in general focuses on defining the terms and specifying definitions of this study.

2.1 Information security

Information security is a daily concern of organizations which handle any type of personal information, health-care data, financial data, or other types of data. In an era where data regarding countless individuals is stored in different kinds of systems, usually not under their direct control, information security becomes a vital component. It is also important to remember that it is difficult to point out when an organization is in a secure state. (Andress, 2014). Therefore, it is natural that information security is commonly discussed theme but still when it comes to the literature, a unified definition of the term cannot be found. In addition, the term is sometimes mixed with IT security or cyber security, and it is sometimes used in a vague way.

Despite the confusion with terms, information security can be discussed with help of two models, which are the CIA triad and Parkerian Hexad. CIA triad is often used when defining information security. Andress (2014) claims that based on CIA triad's principles information security is achieved by implementing different controls, such as managerial or operational controls, that will help deliver information confidentiality, integrity, and availability. According to Raggad (2010) confidentiality is the ability to protect users' or data owner's sensitive information. Integrity refers to the situation where information cannot be modified without permission. Availability means that users have the access to the information any time necessary. Based on these aspects of information security, Raggad (2010) defines information security as the protection of information resources against unauthorized access. Hence, information's confidentiality, integrity and availability are tightly connected to the information security in general.

Parkerian Hexad provides more complex variation of the classic CIA triad. Parkerian Hexad consists of confidentiality, integrity, and availability, but the hexad adds possession or control, authenticity, and utility to the CIA triad for total of six principles. In Parkerian Hexad's context possession or control refers to the physical disposition of the systems and media where the data is stored to. Authenticity means that one can be certain of the proper attribution as to the owner of the data. Utility refers to the usefulness of the data. (Andress, 2014). For example, encrypted data can be useful for the rightful owner but useless for the hacker who cannot decrypt the data. When Andress (2014) defines information security, he relies on to the US law and defines information security through it, as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification and destruction". He adds that in essence information security means that companies, organizations, and people want to protect their data wherever the data might exist and to protect systems assets from users who have an intention to misuse it. Overall, information security is seen as a key component of the modern business world (Andress, 2014).

It is important to add that information security refers only to the information itself. Information system security on the other hand includes the people (Theoharidou, Kokolakis, Karyda & Kiountouzis, 2005). People are the users who create, use, modify and delete data and therefore are an important part of security. This study focuses on information security and people but still the term information security is going to be used to describe the whole phenomenon since it is a stabilized term.

2.2 Security threats

Information security means protection of information resources against unauthorized access, use, disclosure, disruption, or modification. The source of these incidents are security threats. A threat is simplistically said a potential violation of the security of a system which will have a negative impact. Vulnerabilities are security weaknesses or even flaws that make a system prone to an attack. An attack is the situation where a vulnerability is exploited to realize a threat. (Oladimeji, Supakkul & Chung, 2006).

Security threats can be categorized in different ways. Loch, Warkentin and Carr (1992) have categorized security threats into different categories. They call this Four Dimensions of Information System Security. Loch et al. (1992) categorized threats based on the threat's source, perpetrator, and intent. Sources for threats can be internal or external. Perpetrator can be human or non-human from an internal or external source. The intent can be accidental or intentional. The consequences of the threat were divided into disclosure, modification, destruction, and denial of use.

Whitman (2003) gave a more detailed version of threat categorization in his article Enemy at the gate: threats to information security. Whitman categorized security threats into 12 categories based on previous literature and interviews with chief information security officers. The 12 categories are:

1. Act of Human Error or Failure (accidents, employee mistakes)
2. Compromises to Intellectual Property (piracy, copyright infringement)
3. Deliberate Acts of Espionage or Trespass (unauthorized access and/or data collection)
4. Deliberate Acts of Information Extortion (blackmail of information disclosure)
5. Deliberate Acts of Sabotage or Vandalism (destruction of systems or information)
6. Deliberate Acts of Theft (illegal confiscation of equipment or information)
7. Deliberate Software Attacks (viruses, worms, macros, denial of service)
8. Forces of Nature (fire, flood, earthquake, lightning)
9. Quality of Service Deviations from Service Providers (power and WAN service issues)
10. Technical Hardware Failures or Errors (equipment failure)
11. Technical Software Failures or Errors (bugs, code problems, unknown loopholes)
12. Technological Obsolescence (antiquated or outdated technologies)

In Whitman's classification one can see similarities with Loch et al's classification since Whitman's 12 classes can be categorized by using Loch et al's Four Dimensions of Information System Security. Loch et al. give more generalizable model of security threats, but Whitman goes more into detail and specific examples. Similar categorizations can be seen in the IS research. For example, Farahmand, Navathe, Sharp and Enslow (2005) identified three threat agents which were authorized user, unauthorized user, and environmental factors. Threats could be used with physical, hardware, software, and personnel techniques (Farahmand, et al., 2005). Overall, categorizations with person and environment-based and physical or software-based threats seem common in IS research.

2.3 Insider threats

Employees have a vital role in the success of any business, but unfortunately, they often are the weakest link in terms of information security. Security issues caused by insiders go beyond security breaches with outsiders. This demonstrates the fact that employees can be a huge threat to the company's well-being. (Briney, 2001). Insider threats can be defined as human behaviour that occurs when a person does not pursue organizational policies for either harmful or non-harmful purposes. (Greitzer et al., 2008). Raggad (2010) notes that users who have been authenticated and admitted into the system may still be dangerous, even if they have been viewed as trustworthy users. These users can initiate unauthorized activities or intentionally do malicious or illegal actions that can possibly compromise system's security. (Raggad, 2010). Insiders can even cause more harm to the organization compared to outsiders, since insiders have a legitimate access to systems and a knowledge of security processes. Humphreys (2008) defines insider threats as employees, staff, management or contractors who take advantage of the system's vulnerabilities, applications and processes for personal gain, sabotage at the corporate, operational or IT level, or for reckless behaviour without harmful intentions.

Insider attacks originate from various motivational sources such as revenge, financial gain, personal grieve or recruitment. The motivation does not necessarily make an insider dangerous, but the fact that they may have an unfiltered access to sensitive computer systems makes them dangerous. (Raggad, 2010). Even if the intentions are not malicious, the consequences of an accident or negligence can be significant. Insider threats are linked to insider vulnerabilities. Insider vulnerabilities threaten the security of the organization's information assets. For example, lack of awareness of the reverse social engineering attacks can result in an information breach by an employee. Therefore, there are many insider vulnerabilities that either by accident or by being exploited are also being considered as an insider threat. (Humphrey, 2008).

2.4 Information security management standards

As discussed in previous subchapter, the CIA model seeks to define and provide information security. This means protecting information by protecting information's confidentiality, integrity, and availability. This approach has led to the emergence of various standards for information security management and standard implementation, which aims to produce unified and proven policies to secure information. Even standards do not designate complete security, according to Posthumus and Solms (2004) standards are a good way to implement globally used security management tools and standards can assist in increasing trust within organization and its stakeholders.

Solms (1999) defines information security management standard by comparing it to driver's license. Like any motor vehicle on a public road needs a valid certificate that indicates that all technical safety mechanisms are present and like any driver operating that vehicle needs a license that indicates that the person knows how to operate that vehicle in a secure way, a security standard indicates that the technologies and users are operating in a secure manner. Furthermore, a third party like a traffic officers or a standard auditing officer will continuously ensure that the technology is functioning well, and the drivers are obeying the regulations. According to Solms, information security management standards can certainly provide the basis to ensure "safe driving on the information superhighway". (Solms, 1999).

One of the most common information security management standards is ISO/IEC 27001 which is used throughout the world by commercial and governmental organizations in all different sizes (Humphreys, 2007). The ISO/IEC 27001 standard provides information security management system's specification. The standard is used globally by small, medium, and large organizations across diverse range of business sectors. The standard claims to be designed in a way where it is flexible enough to be used by every type of an organization. The ISO/IEC 27001 has become the "de-facto" standard for information security management. (Humphreys, 2008). It is one of the best known, most reliable, and most widely used standards (Lambo, 2006).

ISO/IEC 27001 standard's mission is to help organizations create security management system which can be used as a management tool. In practice, the management system consists of a variety of processes and policies as well as security guidelines to manage different security threats. ISO/IEC 27001 is based on an organization's ability to identify and manage risks and that is why threats and risks are displayed a lot in the standard. According to Humphreys (2011) an organization can apply for an ISO/IEC 27001 certificate from a third party to demonstrate compliance with the standard. The certificate proves that the functions and different parts of the target organization meet the standard's requirements (Humphreys, 2011). ISO/IEC 27001:2017 standard includes ten requirement areas which must be fulfilled to get the certificate. According to ISO/IEC 27001 (2017) the requirement areas are:

1. Scope of the standard
2. How the document is referenced
3. Terms and definitions
4. Organizational context and stakeholders
5. Information security leadership and high-level support for policy
6. Planning an information security management system; risk assessment; risk treatment
7. Supporting an information security management system
8. Making an information security management system operational
9. Reviewing the system's performance
10. Corrective action

In addition to the requirements ISO/IEC 27001 (2018) identifies some critical factors that influence the success of an organization's security management system. Most importantly, the organization must align their security policies and activities with their overall objectives. The organization must have an organization culture-based and systematic approach and framework for security design, implementation, monitoring and development. In addition, ISO/IEC 27001 (2017) emphasizes management’s commitment to information security, so the management system has an actual opportunity to influence and act in the organization. The standard advises to use resources to run security awareness training which is designed to raise awareness and motivation towards the organization’s security policies and practices among employees and critical stakeholders. (ISO/IEC 27000, 2018.)

For increased understandability, ISO/IEC 27001 information security management standard is referenced mostly as ISO 27001 standard in this study.

3 LITERATURE REVIEW

This chapter is divided into three main themes. First in the chapter 3.1 the core research themes of information security are introduced. In chapter 3.2 most applied theories are described. In addition, a projection of these theories related to this research is conducted. In chapter 3.2 a theoretical framework is proposed to capture the dynamic nature of standard implementation process that is being studied.

3.1 Core research themes

3.1.1 Information security policy violation

Although information security procedures are introduced, employees rarely follow them completely regardless of their awareness level (Puhakainen & Siponen, 2010). This may lead to information security policy violations. Information security policy violation in an organizational context is employee's noncompliance with information security policies (Siponen & Vance, 2012). Hu, Xu, Dinev & Ling (2011) define information security policy violations as unauthorized access to data, unauthorized copying confidential data or selling confidential data to a third party. Plainly, information security policy violation can be misuse of organization's systems.

Some ISP violations can be tracked to harmless accidental violations. These non-malicious actions are carried out by an employee, who has no intention to harm the organization or its assets but does so when violating the organization's security policies (Warkentin & Willison, 2009). Some violations on the other hand are caused by employees who are aware of their organizations' information security policies but still choose to violate the policies. These cases are particularly problematic since IS security training and awareness programs may have only little effect on these individuals (Siponen, 2000). In this case an employee intentionally violates the organization's security policy by misusing the privileges they have received (Theoharidou, Kokolakis, Karyda & Kiountouzis, 2005). Employees' information security policy violations have been perceived to increase information security vulnerabilities to the point where over half of all reported security breaches were caused by employees (Puhakainen & Siponen, 2010). These information security vulnerabilities are caused by policy violations and the lack of policy compliance even if policies are specified in organizational documents and guidelines. (Moody, Siponen & Pahnila, 2018).

Many researchers have studied how to explain non-malicious violations in the field of information security research. Guo et al., (2011) have identified characteristics for non-malicious behaviour based on their literature review. The first characteristic is intentionality, which describes that the non-malicious security violation is not caused by an accident like human error. There are conscious decisions behind the act even if it is not meant to be malicious. The second characteristic is self-benefit without malicious intent where the user wants to save money or effort in a way where the violations are noncriminal transgressions. Thirdly, the voluntary infringement is described as users own will to choose to violate the security policies although complying with information system security policies is mandatory. The fourth characteristic is the possibility of causing damage or security risk, where in addition to rule breaking the user also puts organizational information at risk. (Guo et al., 2011). For example, during a hectic time in health care, the employees might share their login credentials because they want to save their own time or leave more time for patient care. The intention is not malicious, but the nurse chooses intentionality and voluntarily to break the rule of login credential sharing even though the person knows it is not allowed. The person might not realize the possibility of causing damage or security risk but still it remains as a possibility.

Non-malicious insiders are overall a substantial challenge for organizations. Guo et al., (2011) argue that information security should be emphasized as business security. According to Guo et al. (2011), more than 14 percent of the CSI survey respondents reported that nearly all losses that faced companies were due to non-malicious but careless behaviour of insiders. It has been argued that non-malicious security behaviour is often a result of weakly implemented information security policies (Jouini, Rabai & Aissa, 2014). Siponen and Vance (2012) refer to some studies when stating that no information security practice or technique can be ultimately successful if it is improperly implemented by its users. The implementation process plays a crucial role when one tries to determine the future of information security policy compliance.

3.1.2 ISP Compliance

Information security policies address concerns regarding security policy violations (Roode, 2018). IS policies give resolutions on actions which are considered inappropriate or appropriate by employees (Baskerville & Siponen, 2002). Security policy may specify what end users should and should not do with organization's information security assets and it may even state the consequences of policy violations (Guo et al., 2011). Like mentioned before, ISO/IEC 27001 standard encourages to run security awareness training which raises awareness and motivation about security policies. Yet the policy is only effective if the employees comply with it. Moody, Siponen and Pahnila (2018) demonstrated empirically that many employees do not follow the security policies even if they are aware of them. However, securely behaving employees make a more secure organization. Siponen (2000) demonstrated how training seems to have only a little effect on malicious insiders. With the non-malicious insiders, the compliance may depend on other things.

Employees compliance behaviour can originate from employee's motivation: more closely from intrinsic motivation or extrinsic motivation. Intrinsic motivation comes from within the individual and this kind of motivation usually leads to behaviour which is rewarding for the person themself. Instinct motivation factors can be enjoyment, interest and meaning. On the other hand, extrinsic motivation results from outer sources. Extrinsic motivation factor can be rewards, punishments, or competition. (Zinatullin, 2016, p. 89). Jai-Yeol (2011) found out that security policy compliance approaches relating to the intrinsic motivation paradigm led to a significant increase in compliant employee behaviour over approaches that handled the extrinsic motivation model. The challenge is that it may be easier to influence employees' extrinsic motivation factors through rewards and punishments than it is to influence intrinsic motivation factors when it comes to security policy compliance.

Zinatullin (2016, p. 87) says that inconvenience is the main driver for user's non-compliant behaviour since users are doing cost-benefit calculations all the time. This phenomenon could be described with an example where user clicks on "you have won the lottery" -link because the excitement of a possibility of an actual win exceeds the inconvenience of the ignoring the warning messages they have been taught. According to Zinatullin (2016, p. 87) in this kind of scenario the decision made was reasonable to a person even if it was not a secure one. This kind of inconvenience driven behaviour can be seen everywhere when people do not lock their computers when leaving to restroom or when they write their passwords down on a post it note since they might feel it is too inconvenient to remember all their passwords.

Zinatullin (2016) proposes that the solution to security compliance would be the raised costs or lowered benefits of non-compliance. For example, employees could be punished for opening the malicious attachments without running a virus check first. On the other hand, this could tarnish the reputation of the security function if the employees become too scared to open any attachments because of the potential punishment. D'arcy, Hovav and Galletta (2009) found out in their study that the perception of sanctions is more effective in deterring risky behaviour than imposing actual sanctions.

On the other hand, Stanton, Stam, Mastrangelo & Jolton (2005) found out in their study that if the users were told that their use of passwords was monitored and that they would get rewards for the desired behaviour, they more likely complied with the password policies. The users changed their passwords more often and made them more complex. This view is supported by Ramamurthy and Wen (2012) who's study highlighted that enforcing rewards in the information systems security context, could be an alternative for organizations where sanctions do not successfully prevent violation. So, it seems that reward system might be more effective than a fear of punishment. Yet in Stanton et al.'s (2005) study although the employees started to use more complex passwords and changed them more often, the employees also started to write down their complex and frequently changed passwords which led to a new security issue. This proves that information security compliance is a complex issue with no unambiguous answer.

Kirlappos, Beautement and Sasse (2013) identified four main factors that can help in changing the perception of cost-benefit balance more towards to policy compliance. These main factors are communicating the value of security, design, supervision, and sanctioning. Communicating the value of security refers to a situation where everyone understands and accepts culture where information risks awareness is present, and everyone is taught the principles of managing risks. Campaigns should steer away from scare tactics and focus more on the user's security values and goals. Design means that the organization makes sure that all the security mechanisms are working properly and aligned with the demands of employees' primary tasks. Supervision and sanctioning refer to a situation where the voluntary compliance is arising from the organization's informal and formal rules, the employees are trusted and there is a positive atmosphere. However, if employees abuse the trust they are given, they should be punished. To punish these individuals, supervision mechanisms should be implemented. Employees that observe sanctions enforced are less likely try to abuse the trust further. (Kirlappos, Beautement & Sasse, 2013).

Based on the literature, it seems that technical measurements have only a little effect on the information security policy compliance. Most factors are linked to the person's own traits and motivation sources. Still ISP compliance is an important factor when organizations try to fulfil the security standard's requirements since securely behaving employees make the organization more secure. Organizations can have an impact on employees since organizations can try to affect employees' security behaviour with awareness and risk management training, supervision and rewards and punishments. Employees' compliance is not a straightforward issue as Stanton et al. (2005) proved in their research. Employees' information security policy compliance has been studied widely but there are no easy answers to solve the challenges when it comes to information security.

3.1.3 Employees' security behaviour

The motivational factors and reasons for employee's behavioural change related to information security policy violations have been studied widely. In this chapter, studies that explain factors affecting information security management standard implementation process, behavioural change and policy compliance are reviewed. Security standards are often implemented to make the processes more coherent and the employees more obedient but there are multiple other factors that have been proven to affect employees' information security behaviour.

Zinatullin (2016, p. 88) says that some may think that security awareness training is an answer when trying to get the employees comply with the policies. While there is a place for such training, the impact of training seems to be low (Zinatullin, 2016, Siponen, 2000). According to Zinatullin (2016) organizations are on a right track if security awareness training aims to change an organization's culture, since trying to make employees' utility-based decisions stop with training will be doomed to fail. In an ideal situation, standards change the organizational security culture, but the implementation does not always have the desired effect.

Hsu's (2009) study highlighted the possibility of unsuccessful standard implementation and differences between standard implementation experiences between managers and employees. Hsu's study underlined how important effective communication is in an implementation process. Hsu observed a security certification implementation process is an organization and compared management's and employees' impressions of this process. During the process of implementing information systems security certification management's intentions were desirable but the managers did not really have the time to communicate the process to the employees in a thorough way. This led to the situation where employees viewed the managers as a ceremonial-integrators, and they felt that the information security is a responsibility of the IT-department only. Employees felt that the training was ineffective, and they just must comply with the management's expectations. Overall, they felt like they are not involved with information security at all. Hsu's study highlighted how the security certification process's success can be viewed completely differently by the employees and the managers. Hsu (2009) claims her findings can serve as a basis for further studies of how social organizational mechanisms can shape and reshape the interpretations of an organization's members. This could enhance the effectiveness of IS security management in the organization.

Stevens and Brownell (2000) examined standard communication and influencing employees' behaviour in their study. They found out that training is influential, and they crafted guidelines how to get the desired behaviour and ethics communicated to employees. Firstly, desired behaviour might seem a little abstract to employees, so Stevens and Brownell suggest modelling the desired behaviour, so it is easier to understand what the employees are being asked to change. Secondly, they suggested that employees should be encouraged to peer-to-peer coaching since it can positively affect employees' behaviour. Thirdly, controls and ethics should be distinctly addressed during training periods as well as on daily basis. Standard related codes should appear clearly in manuals and other documents and they should be easily accessible. (Stevens & Brownell, 2000).

Some suggest that punishments will keep people on the lawful path. In the previous research literature, Pahnila, Siponen and Mahmood (2007) found out that sanctions seemed to have no remarkable effect on the employee's intention to comply with the information security policies. In addition, rewards did not seem to have any effect on information security policy compliance either. On the other hand, peers' and top managers' information security policy compliance seemed to influence the normative beliefs in organizational culture. (Pahnila, et al. 2007). Therefore, top managers should really emphasize the importance of the ISP and act in a desirable manner as an example. It seems that standards and policies should be justified to the employees to make them involved.

Chan, Woon & Kankanhalli (2005) seemed to have a same perception of top managers involvement's importance in employees' information security compliance. In their study they found out that different factors affect the employees' impression of the organization's security climate and as a result employees' compliance too. Based on the study, it seems that employees influence their peer's perception of organization's security climate. Chan et al. (2005) suggest that on daily basis top managers should ensure that employees apply security practices in their daily work, so the information security climate improves and the peer-to-peer support advances.

Van Bruggen, Liu, Kajzer, Striegel, Crowell & D'Arcy (2013) studied how to affect employees' smartphone locking behaviour which is a type of security behaviour as well. Since many organizations allow personal smart phones in organization's networks, it introduces a new kind of a security risk for an organization. Since the device is not owned by the company, monitoring it, and enforcing organizational security policies becomes challenging. In these situations, ability to guide user security behaviour becomes essential. The authors tried to guide behavioural change through messaging which was related to morality, deterrence, and incentives. They found out that appeals to morality were the most effective method over time. For an immediate reaction, the deterrence was the most effective one. It turned out to be difficult to change the behaviour of the individuals who did not protect their mobile devices in the first place. (Van Bruggen et al. 2013). This study supports the theory of users cost-benefit calculations. Like Zinatullin (2016, p. 87) stated, inconvenience is the main driver for user's non-compliant behaviour. In this case the user would have lost one to two seconds every time the user used their mobile device. By communicating morality and deterrence, it may be possible to influence perspectives of cost-benefit-calculation.

Previous studies are versatile, and a lot of different theories have been examined and tested in practice. Still the practical side of the research is lacking and especially the conflicts between standards and reality and change process of information security culture has not been widely studied. It is important to demonstrate how standard based changes in information security policies can affect the employees' daily work and organizational culture.

3.2 Most applied theories

In this chapter the focus is on information security behaviour theories. These theories were chosen based on a literature review. In the literature review these theories were often referred to and applied the most. Theory selection for this study was mostly based on Moody's, Siponen's and Pahnila's (2018) study where they compared the most used theories in information security studies and created a unified model of information security policy compliance. Moody, Siponen and Pahnila's selection of theories was well motivated, and selection's validity was well justified. Not all the theories of the unified model were included since they were not relevant for this study's themes. In addition, one theory was added to direct the perspective towards the empirical study's context. The reasoning behind this selection is discussed shortly in the subchapter 3.1.

The purpose of this chapter is to provide knowledge of the current information security behaviour research. It is important to investigate what the previous research has found and utilize that information in this study if possible. The theories examined are from psychological and criminological fields since the information security policy compliance is often overviewed from these perspectives.

In this study, the conflict between ISO 27001 requirements and practical demands in an organization is observed. Employees' experiences of the standard implementation and the possible changes in IS policy compliance are under observation. The employees' perspective is under study and therefore employees' policy compliance related theories are important foundation for this study. Theories of information security research can offer insights to employees' views and experiences of the old and new security processes and compliance. Especially the general deterrence theory is under inspection since ISO 27001 requires disciplinary actions even some organizations may find them unsuitable.

Some IS theories were left out and one theory was added to the theoretical research. The theories that were left out from Moody et al. (2018) unified model were Neutralization theory, Health Belief Model, Theory of Interpersonal Behaviour, Parallel Processing Model and Theory of Reasoned Action. These theories were left out based on the discussions with the target organization and the literature review. Neutralization theory has been studied a lot, but it does not quite fit to this study's scope where the experiences of information security practices' changes are to be understood. Health Belief Model was not necessary to include since other theories like Protection Motivation Theory has similar main constructs as costs, rewards, and severity related to the scope of this study. Parallel Processing Model was also left out since its focus has been on public health and it has similar main constructs with Theory of Protection Motivation. In addition, Theory of Reasoned Action was left out since Rational Choice Theory and Theory of Planned Behaviour cover these constructs and intention predictors from this study's perspective.

One theory was added to direct the theoretical framework to fit to the need based on discussions with the target organization. The theory that was added was Moral Foundations Theory. The target organization is a Finnish company and Finnish people are known to have high work morality according to the studies: for example, a study conducted in Finland found out that after felonies against human life and physical integrity Finnish people thought most unanimously that calling work claiming to be sick when you are really not sick is morally the most blameworthy thing to do (Berner, 2011). In addition, in literature review it was found out that according Van Bruggen, Liu, Kajzer, Striegel, Crowell & D'Arcy (2013) pleading to morale is an effective way to affect employees' information security compliance. Thus, the moral aspect must be taken more into account in the information security research and that is why The Moral Foundations theory was added.

3.2.1 General Deterrence Theory

Deterrence theory is originally a psychological theory about controlling individual's behaviour through fear of punishment (Gibbs, 1975). Gibbs (1975) argues that the stronger the severity and certainty of sanctions are for unwanted behaviour the more individuals are deterred by it. According to D'Arcy and Herath (2011) the higher the risks, e.g. for punishments are the more likely the person does not commit the crime. D'arcy, Hovav and Galletta (2009) state that individuals calculate the likelihood of getting caught and possibility of consequences before deciding whether to break the rules or not. Based on this logic, users would make less violations if the punishments were more severe. According to D'Arcy and Herath (2011) Deterrence Theory is one of the most used theories in employees' information security behaviour research. It has been used to predict employees' behaviours in different situations. In the context of information security, behaviours have been supportive or disruptive. (D'Arcy & Herath, 2011).

Deterrence theory is indeed present in many studies related to information security behaviour. Some studies have shown that employees follow information security policies more likely if the punishments for misbehaviour or carelessness are severe. In turn, D'arcy, Hovav and Galletta (2009) found out in their study that the actual sanctions are not as effective as the perception of sanctions in deterring risky behaviour. An interesting finding came up from the Herath's & Rao's (2009) study. They found out that certainty of sanctions had a positive impact on employee's intention to comply with the information security policy, but they also found out that severity of sanctions had a negative impact on security behaviour intention. (Herath & Rao, 2009). In addition, methods based on the deterrence theory effect employees' extrinsic motivation which can have a negative impact on their intrinsic motivation. As previously discussed, intrinsic motivation affects employees' behaviour more.

Deterrence theory has been criticized since it does not apply in all situations. According to Pahnila, Siponen and Mahmood (2007) sanctions seemed to have no significant effect on the employee's intention to comply with the information security policies. Hu et al. (2011) found out that deterrence had no significant effect on the employees' intentions with information security policy compliance. Kankanhalli, Teo, Tan and Wei (2003) introduced similar issues since consequences for information security violations may not as severe as punishments for other crimes. Although there is criticism for the deterrence theory and the results from the studies are not consistent, the theory is included to this study since ISO 27001 requires disciplinary actions to be documented and communicated to employees.

3.2.2 Rational Choice Theory

Rational choice theory is a framework for understanding social and economic framework of human behaviour and it is one of the dominant theories concerning human behaviour. The core of the theory is people's aim to maximize their personal benefits while minimizing their costs. According to Rational choice theory, personal gain tends to be human's main motivator. (Blume & Easley, 2008). People perceive benefits and costs of the outcomes and act according to their calculations. Rational Choice Theory offers a lens to how employees are making decisions whether to comply or not to comply with information security policies. According to this theory, it might be rational for employees not to comply with the policies since the effort it takes can outweigh the perceived risk reduction level. (Zinatullin, 2016).

Aytes and Connolly (2004) believed that individuals' safe computing behaviour is a rational choice based on the perceived usefulness of the safe behaviour and the possible consequences of not behaving safely. They assumed that an user faces two choices whether to use safe practices which will not lead to negative outcomes but costs time and effort, or to use unsafe practices which does not cost resources but can possibly lead to a negative outcome. (Aytes & Connolly, 2004). This is a simplified model since even safe computing behaviour can lead to a negative outcome. Hackers can attack a user's computer even if they are acting carefully or some website can leak a user's password even if the user has a complicated password.

According to Aytes and Connolly (2004) behind the rational choice are different factors which affected the choice: training, media, co-workers, friends, policies, and experiences are all influencing in the background. These factors in the background lead to awareness of safe practice and negative outcomes. In addition, three factors affecting the rational decision are availability of the safe practice option, perception of the probability of negative consequences and the perception of the severity of the negative consequences. It comprehends to add that Aytes and Connolly (2004) found out that users will not change their behaviour through only providing them more information about safe practices and computing risks. Therefore, the informational training is not enough when trying to affect employees' secure computing behaviour.

3.2.3 Theory of Self-Regulation

Bagozzi (1992) has formed a Theory of Self-Regulation based on Theory of Reasoned Action, Theory of Planned behaviour, and Theory of Trying. Bagozzi expands theory of reasoned action by adding desires. Desires are defined as cognitive or emotional inclinations that direct how one behaves (Bagozzi, 1992). Bagozzi explains human behaviour through self-regulatory processes which are monitoring, appraisal and coping activities. These processes translate attitudes into intentions, subjective norms into intentions and intentions into actions leading to goal attainment.

Bagozzi (1992) states that attitude toward action is not the only factor that might influence behaviour. Theory of Self-Regulation explains how individuals might have a social normative pressure and positive attitude towards behaviour but if desire is not consistent with behaviour, the behaviour might not take place.

Bagozzi (1992) defines theoretically a desire as a cognitive or emotional tendency to how an individual behaves. Further, desires become important when there are other objectives which may have a higher priority to the individual. Moody et al. (2018) links the Theory of Self-Regulation through how an individual can self-manage security goals based on thoughts and emotions. They mention that even the theoretical explanation about desire affecting behaviour is richly explained, it has not been studied a lot in the context of information security behaviour.

3.2.4 Protection Motivation Theory

Protection Motivation Theory examines how individual's perception of threats and coping with them can influence decisions to engage in defensive behaviour. Protection Motivation Theory is a well-established approach in the health behaviour domain, and suitable for behavioural interventions (Williams, Noyes & Warinchi, 2018). Over time, the theory has been extended into the information security studies. The primary points of Protection Motivation Theory according to Williams, Noyes & Warinchi (2018) are:

- the perceived severity of a threatening scenario
- an individual's perceived vulnerability to that scenario
- the perceived efficacy of the protective behaviour in reducing vulnerability to that scenario
- the perceived individual's ability to engage in the relevant protective behaviour.

Protection Motivation Theory has been applied into studies about individual intentions to engage in security behaviour. These four aspects introduced were found to influence intentions in different contexts like use of home wireless security (Woon, Tan & Low, 2005), anti-spyware software adoption (Chenoweth, Minch, & Gattike, 2009) and anti-virus software use on mobile devices (Al-Ghaith, 2016).

According to Herath and Rao (2009) in the information system security context, Protection Motivation Theory can be visualized in terms of an employee's assessment of the consequences of the security threat and the probability of exposure to a substantial security threat. Fear arousal is the level to which an employee believes the organization's information assets are threatened. If the employee perceives possible damages or disturbances relevantly severe, they are more likely to be concerned about the threat. To the contrary if an employee does not believe that an employee is facing a factual security threat, they are less likely concerned. (Herath and Rao, 2009). Thus, in the information security context Protection Motivation Theory means that if the employee sees the threat as an actual concern, they more likely have a positive attitude towards protection mechanisms like security policies.

Based on the Protection Motivation Theory intervention messages can be tailored to maximize the likelihood that a user will engage in a desired protective behaviour. Messages can be framed to potential gains or potential losses when engaging in a protective behaviour. These messages can be tailored even to different personality types depending on if the employee is more sensitive to gains or losses. Use of these kinds of messages framing with different personalities based on Protection Motivation Theory needs to be further studied in the context of cyber security. (Williams, Noyes & Warinschi, 2018).

3.2.5 Theory of Planned Behaviour

The theory of reasoned action can be considered a precursor to the theory of planned behaviour. The core of the Theory of Planned Behaviour is the individual's intention to perform a behaviour being discussed. Intentions capture the motivational factors that influence an individual's behaviour. Intentions are indications of how hard individuals are willing to put in effort to behave in a certain way. (Ajzen, 1991). Ajzen states that the general rule is that the stronger the intention is, the more likely the performance is going to happen. It should be noted that these behavioural intentions happen only if the individual can decide to perform or not to perform the behaviour. In most cases some security behaviour e.g. password use is not voluntary. Ajzen (1991) adds that in addition to intentions, non-motivational factors like time, money, skills, and cooperation of others affects performance. If an individual holds required opportunities and resources, and intends to perform the behaviour, the individual should succeed in it. Simply, behavioural achievement depends on motivation as in intention and ability as in behavioural control.

The theory of planned behaviour places perceived behavioural control with behavioural intention into an equation predicting behavioural achievement. Ajzen (1991) introduces two rationales for this. The first one is holding intention constant, the effort expended to bring a course of behaviour to a successful conclusion is likely to increase with perceived behavioural control. For example, if two employees want to achieve a good level of safe computing practices, the one who confidentiality believes in their own capabilities and success, will be more likely to learn and succeed.

The second rationale is according to Azjen (1991) perceived behavioural control can often be used as a substitute for a measure of actual control. To the extent that the perceived control is realistic, it is useful in predicting the probability of successful behaviour. If one wants to change an individual's behaviour intention, perception of behavioural control, attitude towards the behaviour and subjective norms are great opportunity points to influence. (Azjen, 1991). In an organization's security context this could be translated to an attempt to influence the employee's intention to comply with the security policies instead of the actual behaviour. Also, the organization's general attitude towards information security and compliance could affect the employees' intentions to comply and behave securely. That is why organizations should encourage their employees to act securely by the means of information security policies. Employees should possess the required resources and knowledge before asked to perform properly.

3.2.6 Control Balance Theory

Control balance theory is a theory proposed by Tittle in 1995. The core of this theory is that individuals do deviance or crime because they need to return the state of control balance or extend their own control over other individuals. Control balance is the ratio of control that others exert on the individual or the control individual exerts over others. (Tittle, 1995). Tittle (1995) introduces two situations where the control is unbalanced: control surplus and control deficit. If a person has control over a surplus, the person has more motivation to continue to control others and thus increase their control surplus. If a person feels that others have more control over them than the person has on their life, the result is a control deficit which will lead to a submissive deviance. Deviant behaviour allows the person to exert more control and to try to balance the control in their life. (Tittle, 1995). For example, an excess of control can cause an individual to entrust their subordinates with questionable tasks related to information security. In a deficit situation an employee who feels like they do not have control of their life, might execute ransomware attacks towards authorities to feel more in control.

Control Balance Theory proposes that violation motivation will increase the intention to violate a policy. The violation motivation will increase further when the individual is told about their control imbalance. Also, the deviance will continue only if there are no constrains that deters the individual. (Moody et al. 2018). Even the Control Balance Theory is a criminological theory like Deterrence Theory, it has not been widely used in any information security research before Moody et al.'s (2018) study of information security compliance's unified model.

3.2.7 Moral Foundations Theory

Some employees might follow the security policies since they feel it is just morally right thing to do. In fact, morality influences information security policy violation according to Siponen and Vance (2012) and Pfleeger, Sasse and Furnham (2014). Morale's influence can be traced to Haidt (2012) who created the Moral Foundations Theory. This psychological theory tries to explain the origins of human moral reasoning and the variations in it. Moral systems are interlocking sets of values, virtues, norms, practices, identities, institutions, technologies, and evolved psychological mechanisms that work as one to overcome or regulate self-interest and make cooperative societies achievable. (Haidt 2012).

Individuals often assume that morale means fulfilling one criterion first which is do no harm to others. People can feel like they are not doing anything wrong if they are not harming organizational or employee security, but the challenge is that people's moral systems differ. (Pfleeger, Sasse & Furnham, 2014). What might be morally correct to one person might be foul for others. Haidt (2012) proved in his empirical research that morals are multi-faceted, guiding people's choices and behaviour and can be divided into six dimensions:

- Care versus harm
- Fairness versus cheating

- Liberty versus oppression
- Loyalty versus betrayal
- Authority versus subversion
- Sanctity vs degradation

Pfleeger et al. (2014) state that if the moral profiles of individuals are known, it can be possible to see where they stand on these six dimensions and how the position relates to positive security culture. Different dimensions of moral foundation are linked to different security challenges, triggers, and actions. For example, Pfleeger et al. (2014) suggest that in the dimension of liberty versus oppression the challenge is the freedom to act but within organizational policies. The security triggers are reminders about the security policies. Security actions linked to liberty versus oppression are effective communication, enforcement of security policies and integration of policies into business practices. Pfleeger et al. (2014) suggest that the awareness and training can be improved if organizations can take advantage of each employee's predispositions to perceive and react. However, it must be considered that not all organizations have resources to study employees' moral dimensions.

3.2.8 Summary

Based on the literature review it can be stated that employees' information security behaviour and compliance has been widely studied. The literature reviewed displays that human behaviour cannot be explained by one theory only. Multiple factors affect employees' intentions and behaviour. In example, motivation, intentions, morale, organizational culture, punishments, and benefits can all affect the employees' compliance. Studied theories were from the fields of criminology, psychology, and social psychology. Many different viewpoints are available when studying employee's behaviour but the theories from these fields seem to be most often used in information security research. In the table 1 the reviewed theories are summarized, and the main factors are introduced.

Theory	Factors	IS example	References used
Deterrence Theory	Formal control Informal control	Sanctions to employee who break the IS policy might prevent future noncompliance.	Gibbs (1975) D'arcy, Hovav and Galletta (2009) D'Arcy and Herath (2011) Herath and Rao (2009) Pahnila, Siponen and Mahmood (2007) Kankanhalli, Teo, Tan and Wei (2003) Hu, Xu, Dinev and Ling (2011).
Rational Choice Theory	Formal control Informal control	Employees safe computing behavior is a rational choice based	Blume and Easley (2008)

		on the perceived usefulness of the safe behavior and the possible consequences of not behaving safely.	Zinatullin (2016) Aytes and Connolly (2004)
Theory of Self-Regulation	Attitude Desire Subjective norms	How an individual can self-manage security goals based on thoughts and emotions.	Bagozzi (1992)
Protection Motivation Theory	Costs Response-efficacy Rewards Self-efficacy Severity Susceptibility	Employee's assessment of the consequences of the security threat and the probability of exposure to a substantial security threat.	Williams, Noyes and Warinchi (2018) Herath and Rao (2009)
Theory of Planned Behaviour	Attitude Perceived behavioural control Subjective norms	Organization's general attitude towards information security and compliance could affect the employees' intentions to comply and behave securely.	Ajzen (1991)
Control Balance Theory	Constraints Control balance Situational provocation Violation motivation	Control surplus can lead to e.g. pressing others to behave insecurely. Control deficit can lead to e.g. ransomware attacks against authorities. Violation motivation will increase the intention to violate a policy.	Tittle (1995)
Moral Foundations Theory	Care vs harm Fairness vs cheating Liberty vs oppression Loyalty vs betrayal Authority vs subversion Sanctity vs degradation	Employee's moral dimension position relates to organization's positive security culture.	Haidt (2012) Pfleeger, Sasse and Furnham (2014)

TABLE 1. Summary of the reviewed theories.

Despite extensive research of information security behaviour theories, none of the studied theories seem to be suitable to capture the dynamic nature of policy implementation with its contextual richness. These information security theories focus on people's security compliance in such a narrow way which does not include organizational changes, processes, and experiences. The complexity of the standard implementation cannot be handled through individual theories that leave out all the contextual factors. Based on these theories it is not known how information security management standards affect employees' security behaviour in daily work and what kind of conflicts might appear between the standard requirements and practical demands in employees' work environment.

An investigation of how the conflict between standard requirements and practical demands is resolved and how employees have experienced these practices and changes that have taken place in the implementation process is needed. The aim of the empirical study is to extend information security studies from individual theories to deeper understanding of the context and content of the implementation process. The duality between standard requirements and real-life practices and demands must be emphasized in the information security research. Therefore, none of the reviewed theories seem adequate to answer the questions that arise related to the information security management standard implementation process. From the reviewed IS theories the deterrence theory is determined as a one interview theme, since the new information security practices are based on ISO 27001 which requires disciplinary actions. The target company's representative argued that disciplinary actions do not fit into a Finnish organization where trust and leadership are core principles of the organizational culture. Regardless, all the studied theories are reflected when analysing the results. A contextual framework is proposed in the next chapter to capture the nature of the standard implementation process and employees' experiences of it.

3.3 Theoretical framework

Since ISO 27001 standard implementation is dynamic in nature with its contextual richness the reviewed theories are not suitable to capture the whole ISO 27001 implementation process that might have many consequences in employees' daily work and security behaviour. The organization's history, corporate acquisition and employees' experiences all affect the standard implementation and information security policy compliance related to it.

Soliman and Rinta-Kahila (2020) developed a framework to emphasize the importance of process, content, and context of the research. They described their framework to have resemblances with Pettrigrew's contextual approach. Contextualist analysis is often used to understand organizational change in empirical research (Soliman & Rinta-Kahila, 2020).

The differences between process, content and context are useful for analysing the different aspects of the multidimensional ISO 27001 implementation process. To deeply understand this process and the changes following it, a contextual approach is proposed to work as a theoretical framework for this study. The three parts of the contextual framework are shortly described in the following subchapters. In addition, their relation to this study is briefly discussed. The theoretical framework is used when analysing and presenting results of the empirical research.

3.3.1 Process

Process describes the stages through which change occurs. According to Pettigrew (1985), in a contextual sense, a process means interdependent, sequence of actions and events, which is being used to explain the origins, continuance, and outcome of some phenomena. The Dialect Process model describes a conflict until a resolution is reached in the form of synthesis. (Pettigrew, 1985). To resolve the conflicts between ISO 27001 requirements and practical demands and special demands of software development, a synthesis is needed. The process can be divided into three different stages: before ISO 27001 implementation, during implementation, and after implementation process as in maintenance phase. The stages are constructed through the interviews where the interviews are held before and after the ISO 27001 auditing.

3.3.2 Content

Content describes what happens in each stage of the process and how the phenomenon changes (Soliman & Rinta-Kahnila, 2020). The attitudes, triggers to move to the next stage, forces that hinder such movement are included in the content part. The content in this study is seen as the decisions that the target unit in different stages related to the standard implementation, how the conflicts were resolved and how it changes the perception of the information security in the organization.

For example, Deterrence theory suggests that fear of punishments keep individuals from breaking the rules. In this study, the punishments or disciplinary measures are content conceptualized in a way where the employees' perception of the punishments in different stages and actions related to the resolution in different stages are observed.

3.3.3 Context

Soliman and Rinta-Kahnila (2020) describe context as the organizational environment and the background story in which the changes are happening. They add that "It should be noted that "context" is a debatable concept that can refer to various things, including geographical context (place), temporal context (time), and cultural context (history), to name a few". Soliman and Rinta-Kahnila note that if the research is abstracted too close to the context, it can lead to local truths which limits the findings' transferability. They made an excellent remark about theorizing which needs a balance between context-specificity and universalism. Overall, context can give the change process frames that help in understanding the situation and phenomenon more deeply.

The study's context is clarified through the interviews. The goal is to find the context where the process and content are taking place. Since the subject is a software development unit to a in a company which already has the ISO 27001 implemented and certified, the context can be the software company and the target unit and their relations. These aspects lay more on a cultural context than geographical context or temporal context. Temporal context is still valid since the corporate acquisition has already taken place and the ISO 27001 implementation is studied throughout different and individually captured moments.

4 EMPIRICIAL RESEARCH

Siponen (2006) argued that standards consider the question “what”, not “how”, and the previous research seemed to have similar deficiency when it comes to standard implementation. Standard implementation is dynamic in nature and it needs to be studied extensively. The aim for this research is to understand how the target unit is going to handle conflicts between ISO 27001 standard’s requirements and demands of daily work, and how employees are experiencing the implementation process and changes in security practices. As the study tries to understand this phenomenon, a qualitative research method is justified in answering the main research questions:

- Q1: How employees experience the ISO 27001 standard’s implementation in a software development environment?
- Q2: What kind of conflicts might appear between ISO / IEC 27001 standard requirements and day-to-day work?
- Q2: How the target unit resolves the conflicts between ISO / IEC 27001 standard requirements and day-to-day work?

Earlier chapters sought to explore the research question by looking at the previous literature on the topic. It was clarified how the individual theories are not enough in trying to understand these conflicts and experiences in practice. In the following chapters the research questions are examined by executing an empirical research. Chapter 4 is organized in a following way: chapter 4.1. introduces the research methods and the goal of this research. Chapter 4.2. describes how the data was collected for this research. In chapter 4.3. the target organization of the research is described, the interviews and the interviewing process in described and the analysis method is discussed.

4.1 Research method

The study uses a qualitative approach to gather rich qualitative data to answer the research questions. According to Darke, Shanks and Broadbent (1998), qualitative approach is better for understanding the phenomenon in its natural context compared to the use of quantitative approach. This research aims to increase the understanding of the information security management standard implementation and possible challenges from employees’ perspective. According to Eisenhardt and Graebner (2007) a case study is a particularly valid research methods when there are no established theories on the topic.

This research is a combination of exploratory and descriptive research, with a constructive research approach. Exploratory research seeks new perspectives, finds new phenomena, and explores little-known phenomena. Descriptive research documents the central, interesting features of the phenomena. Efforts have been made to limit and keep the research problem clear and narrowed, but preparations are being made to refine its layout as the research progresses since qualitative research requires flexibility in problem solving.

This study adopts a longitudinal research design where the same individuals are examined repeatedly. One of the goals of longitudinal studies is to find any changes that have occurred between the interviews and understand the phenomenon better through these changes. A prospective study approach was selected in which group of subjects are chosen and followed over time. With longitudinal research design it is easier establish the real sequence of events and understand them through the chosen contextual approach. The longitudinal study enables following the process, content, and context through different stages of change. In addition, prospective longitudinal studies reduce the risk of recall bias, or the difficulty to recall past events correctly.

In addition to longitudinal research design, this study uses single case design. According to Saaranen-Kauppinen and Puusniekka (2006) a thorough examination of an individual case study can provide information that goes beyond the individual case, although it does not allow generalization. Eisenhardt (1989) states that random selection of cases is not recommended in case studies even if it is possible. This study is a single case study, so the organization was not randomly selected. As the focus is on the change process, it was important to work with an organization which is going through a policy change. In accordance with the guidelines of Benbasat et al. (1987), two data collection methods are utilized in this case study. The methods used are interviews and documentation.

Interviews are used to gain relevant data. The purpose of the interviews is to increase the validity of the research by ensuring that the research results produced are correct and aligned with the IS research. Interview aspect is also considered important in the study because it is crucial for the research topic to understand the phenomena from the employees' perspective. When interviews are used for research purposes, it is essential to understand that the interview serves as a systematic form of data collection and aims to obtain the most reliable information possible.

The study uses a semi-structured interview method. A semi-structured interview is also called a theme interview, in which the interview is clearly focused on specific themes and is not structured around detailed questions (Hirsjärvi & Hurme, 2001, pp. 47-48). Theme interviews are applied in such a way that in addition to clear themes, certain core questions are prepared for the interview that require interpretation, but at the same time the interviewee is given enough space to add to the themes. The theme interviews are also characterized by the fact that the researcher has the opportunity to deepen the discussion on the basis of the subject areas as required by the research interests (Hirsjärvi & Hurme, 2001, p. 67). Two interview rounds are held during a cycle of three months to capture the change process which comes with the ISO 27001 implementation. Semi-structured interviews are conducted by recording and transcribing the interviews. Literally transcribing is not considered necessary and often subject interviews are transcribed by theme, which is possible because the researcher knows his/her material well enough and identifies the essentials of the recording (Hirsjärvi & Hurme, 2001, p. 142).

In this research, 10 employees are being interviewed. More than 15 interviews would become a resource challenge since one interview hour takes about 6-12 hours to transcribe (Saaranen-Kauppanen & Puusniekka, 2006). In qualitative research, the goal is often to understand a phenomenon, not to find statistical links. Qualitative research makes possible that the research material does not have to be large and sometimes even a single case may be sufficient (Saaranen-Kauppanen & Puusniekka, 2006). Qualitative research is about discretionary sampling. This means that usually the data and subjects are selected based on criteria set by the researcher. When research material is collected from people, subjects can be searched, for example, with the help of existing contacts, so-called snowball technique. (Saaranen-Kauppanen & Puusniekka, 2006). In this research the interviewees will be collected through contact person in the target organization. Interviewees will be organization's employees who have worked in the organization while ISO 27001 implementation and auditing process.

Interview data will be analysed by transcribing the interview records. Transcripts will be colour coded to spot different or frequent themes. This kind of coding helps the researcher to piece together which parts of the research data are about the same topic (Saaranen-Kauppinen & Puusniekka, 2006). This kind of approach is called thematic analysis which will be conducted. Coding and quantification can be used based on examples in unifying themes. Type reports can also be used to create themes: the content of types (descriptions or narratives) containing typical elements can be further specified through themes, or it is possible to move from theme design to typing. Thematic analysis is especially suitable for analysing data from interviews, where the interview structure has been built on themes. (Saaranen-Kauppinen & Puusniekka, 2006).

Sarajärvi and Tuomi (2017) point out that a core point of qualitative study is subjectivity. Researcher's objective perceptions are included in interaction with the interviewees. That is why it is important to provide detailed description of the data gathering and analysis process.

4.2 Data acquisition

The data for this research was gathered from interviews conducted with the employees of the target unit. Interviews are an important source of information in case studies (Darke et al. 1998) and therefore interviews were used as the primary method for empirical data acquisition. Interviews provide an opportunity to deeply understand the thoughts and views of the interviewees related to the research question. There is a risk of distortion in interviews since the thoughts and views are always subjective. One way to avoid this distortion is to use multiple interviewees (Eisenhardt et al. 2007). Therefore, multiple interviewees were used from different positions in the target unit. Different interviewees can give different viewpoints to the phenomenon (Eisenhardt et al. 2007). Theme interviews give an opportunity to specify interesting topics arisen during the interviews. This can enable to further understand the phenomenon and to answer the research questions. Since the questions are about experiences, theme interview suited the occasion better compared to other interview methods. Interviews were expected to produce varying responses depending on the interviewees.

Since the research is about the change process, longitudinal study is necessary. First interviews were held before the ISO 27001 audition took place and the security policy was changed. Second round of interviews for the same interviewees were held after the ISO/IEC 27001 certificate authority auditing was finished and three months has passed, so the employees became more familiar with the new policy and practices. Both interview rounds were theme interviews, but the second interview round questions were altered based on the findings of the first interview round. The interview questions were not given to the interviewees beforehand, but they were informed in advance of the topic which were to be discussed. The interviews were carried out in Finnish. The term definition challenges were solved by asking the interviewees to elaborate their answers and informing them that they can ask the interviewer to elaborate or readjust the questions.

The aim of the interviews was to find out the experiences of the change process and conflict resolution that took place when the target unit implemented the ISO 27001 based security standard. In addition, the disciplinary measures were under inspection since the ISO 27001 standard requires including them into the security policy. The themes of the interview included questions about what employees know about current practices, are there areas involved in day-to-day work that they find most relevant, which areas are perceived as impractical or obsolete, how they experience their compliance, what their thoughts about ISO 27001 implementation are, has there been any challenges and how disciplinary actions were perceived. Themes were chosen to understand the change process as fully as possible and to understand the experiences and perceptions the employees have from the theoretical framework's perspective.

The interviewees were divided into two groups in both interviewee rounds based on their job descriptions: employees and managers. Employees were mostly software developers and testers and managerial level employees were managing eleven or more subordinates. The interview themes stayed the same between these groups, but the outlines differed a bit. The interviews were based on the themes that were found from the literature review and on the attempt to answer the research questions. The interview was constructed around these themes:

1. Perception of organization's attitude towards security environment: if it is serious, loose, or something else.
2. Perceived knowledge and familiarity of security policy's content
3. Attitude towards disciplinary actions and the need for them
4. Perception of employees' own policy compliance
5. Motivation to comply with security policies

6. Attitude towards ISO 27001 standard implementation and certification
7. Experiences of the ISO 27001 implementation

Between two interview rounds, the possible changes in the employees' answers is examined. The possible influence of ISO 20071 implementation is observed between the interview rounds.

4.3 Research conduction

In this chapter the process of conducting the research is described more in detail. In chapter 4.3.1 the subject organization is introduced and justified. In the chapter 4.3.2 process of conducting the interviews is described. In chapter 4.3.3 the data analysis methods are introduced and justified.

4.3.1 Research setting

The target organization requested to stay anonymous since their area of business is security sensitive. For this reason, it will be referred as pseudo name Securitym. Selection of the target organization for this research was based on its suitability and availability to the research. Securitym is a Finnish organization focusing on ICT services. The organization operates in Finland in the private sector in B2B markets. It acquired a target unit through a corporate acquisition. It had approximately 300 employees in 2020. Securitym's target unit focuses only on software development which differs from the target company's area of business. Securitym has an ISO 27001 certification, but the target unit has not been audited before. Before the target unit could follow their own software development guidelines and processes, and organizational level information security policy, but since Securitym is ISO 27001 certified, they wanted to bring the target unit within the scope of the standard and audit the target unit's operations too. During the interviews, the organization was producing secure development guidelines for software development and system delivery.

4.3.2 Interviews

The interviews were conducted in April 2020 and in September 2020. Ten employees of Securitym's target unit were interviewed. The interviews were transcribed word-to-word in the same day or at latest in the following day. The organization could choose their own interviewees but employees from different positions were requested. The interviewees' backgrounds varied from software development to testing and to management. The interviewee's backgrounds are not further specified to protect employees' anonymity. The interviewees had worked in the organization from 1.5 years to 16 years so everyone was familiar with the organization's policies and processes.

The interviewees were subordinates or managers: 7 of the interviewees were subordinates and 3 of the interviewees were managers. Managers had at least eleven or more subordinates. All the interviews were held individually due to the subject's sensitive nature. Due to the Covid-19 pandemic during 2020 all the interviews were conducted remotely. The platform for the interviews was Microsoft Teams for all the interviews. All interviewees were asked for permission to record the interviews for transcribing. Every interviewee allowed recording.

The length of the interviews varied between 41 minutes to 70 minutes. Since all the interviewees were native in Finnish, the interviews were held in Finnish for more reliable mutual understanding. All the interviews were transcribed in Finnish and the analysis was also made in Finnish. All the quotes in this study are translated from Finnish to English to the best of the interviewer's ability.

The interviewees background was clarified in the beginning of the interviews. The interviewees were asked what their education was, what their position in the company is, how long they have been working in the company and what their general perception of the organization's culture is. This was done to study how much the interviewees differed from each other and if they had background from information security etcetera. Most of the interviewees were engineers from information technology or software development but different educational backgrounds were present too. Most of the interviewees who had background from the technological study fields had had couple of courses related to information and software security in their studies.

4.3.3 Data Analysis

All interview records were transcribed soon as possible after the interviews, usually on the same day. The focus was not on the used language but in the described attitudes, expectations, and thoughts, thus special characters were not used. After transcribing the interviews, a colour coding was conducted. Similar themes, paragraphs and phrases were labelled with selected colours to organize and observe the information. Colour coding helps according to Saaranen-Kauppinen and Puusniekka (2006) to observe which parts in the transcribed data are about the same topics and themes.

The chosen analysis method for analysing the data acquired from the interviews was a thematic content analysis method since it is presumably fit to semi-structured interviews. The thematic content analysis aims for linking the themes and interviews together under category system. Existing theories or frameworks can be used in the thematic analysis, and the thematic analysis was used in that way. (Saaranen-Kauppinen & Puusnieka, 2006). Theoretical framework was used in the thematic analysis. The processes, content and context were separated and studied individually to understand the change process better. The process aspect guided the longitudinal approach where data from different stages was captured and compared to the other stages. Content highlighted the analysis' part of the attitudes and triggers that led the process forward. Context described the environment where the changes were happening, and this was considered in the data analysis. The organizational history and relationship between the target unit and organization was taken into consideration when analysing the interview data. According to Saaranen-Kauppinen and Puusnieka (2006) thematic analysis is particularly well suited for analysing interview data when the interview structure is built on topics. The themes found based on the data mimic the interview structure very closely. The parts of the interviews that were previously coded are then organized into the identified topics.

5 RESULTS

In this chapter the results of the empirical research are presented. The case study aimed to find answers to the research questions which were regarding ISO 27001 implementation conflicts and their resolutions and its influence on employee's experiences. The research questions were:

- Q1: How employees experience the ISO 27001 standard's implementation in a software development environment?
- Q2: What kind of conflicts might appear between ISO / IEC 27001 standard requirements and day-to-day work?
- Q3: How the target unit resolves the conflicts between ISO / IEC 27001 standard requirements and day-to-day work?

This chapter has been organized into two different themes. Chapter 5.1 focuses on general findings considering the information security culture, information security habits and general attitudes towards information security, ISO 27001 certification and the implementation process. The first subchapter tries to build a context to the change process that is occurring during the study. This helps to understand organizational environment and the background story. The organizational context is described before and after ISO 27001 implementation to highlight the changes the standard implementation has brought with it. This gives an insight of the context but also the process of the implementation. In addition, employees' experiences of ISO 27001 implementation are presented. In chapter 5.2 the conflicts between ISO 27001 standard's requirements and the day-to-day work are described and the resolutions are observed. As content describes how the phenomenon changes, the content in this study is seen as the decisions that the target unit and the employees made related to the standard implementation, how the conflicts were resolved and how it changes the perception of the information security in the organization. Two different conflicts related to code reviewing processes and disciplinary measures were captured to give an insight of how information security management standards might not fit straightforwardly into every organizational setting.

5.1 General findings

In this subchapter the general findings of the empirical study are presented. These general findings work as a context of organizational culture and background story for the phenomenon that is being studied. General findings give an overview of the employees and employees' perceptions and attitudes towards information security and ISO 27001 implementation. This works as a context for the findings as well. The changes in these perceptions and attitudes are studied in a longitudinal study. In addition to building the context to the study, it is interesting to see if there have been any changes in the interviewees' attitudes and perceptions. In the following figure, the different stages that are observed in the general findings are presented:

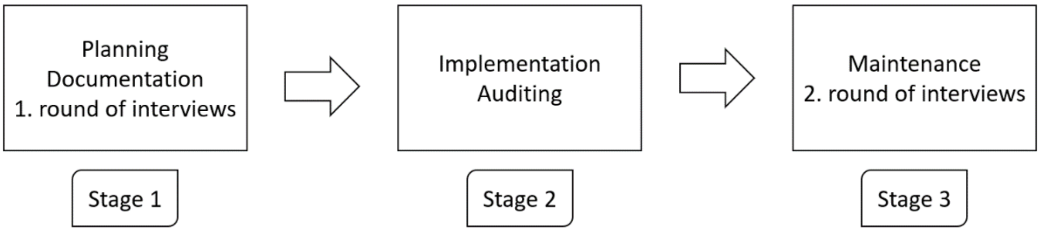

FIGURE 1. Stages of the process

Chapter 5.1.1 introduces background of the interviewees. Chapter 5.1.2 presents the key findings of stage 1 which aims to capture the target unit's state before the ISO 27001 implementation and auditing. Chapter 5.1.3 observes stage 3 which handles the target unit's state after the ISO 27001 implementation. Between the two interview rounds, three months has passed. Chapter 5.1.4 address employees' experiences of the ISO 27001 implementation process and the different stages.

5.1.1 Background of the interviewees

For the empirical study, 10 employees of the organization's target unit were interviewed. The interviewees were both male and female employees. The interviewees had different educational backgrounds but none of the interviewees were information security professionals. Three of the interviewees were managers with 11 or more subordinates and the rest were categorized as employees. The employees were working mostly in software development in different roles. Employees' backgrounds are not further specified since it might make the interviewees recognizable. Since this study is focusing on information security and attitudes which are very sensitive in nature, it is crucial to make sure that the interviewees cannot recognize each other from the quotes and results.

The interviewees are individualized in the table 2 using numbers from 1 to 10. Interviewees' names were replaced with the title "Interviewee". Their working history in Securitym is not specified since it would make the interviewees recognizable. The longest employment was around 16 years and the shortest was around 1 year. All the interviewees have received information security training in some point of their employment.

INTERVIEWEE	POSITION
INTERVIEWEE 1	Employee

INTERVIEWEE 2	Employee
INTERVIEWEE 3	Employee
INTERVIEWEE 4	Employee
INTERVIEWEE 5	Employee
INTERVIEWEE 6	Manager
INTERVIEWEE 7	Employee
INTERVIEWEE 8	Employee
INTERVIEWEE 9	Manager
INTERVIEWEE 10	Manager

TABLE 2. Interviewees' positions

5.1.2 Before ISO 27001 implementation

The state of the security culture and attitudes were studied to give a context and a content to the different stages of the research. The state before ISO 27001 implementation reflects the first stage of the process. To examine the general perceptions and attitudes towards information security, information security policy compliance and ISO 27001 implementation, the interviewees were asked questions related to their experiences and attitudes. The questions were based on the literature review and target unit's development environment. In table 3 the general results are presented in a summarized form. These themes were discussed using the following questions:

1. How would you describe your organization's approach to information security?
2. How familiar are you with current security policy?
3. How security policies are present in your daily work?
4. What motivates you to adhere to your organization's security policies?
5. Do you feel that ISO / IEC 27001 standard certification is necessary? What can it bring with it? How do you think that affects your daily work?

The answers are categorized in the following table to give a quick overview of the general findings of the first interview round:

	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10
MAIN ADJECTIVE DESCRIBING INFORMATION SECURITY CULTURE	Serious	Serious	Strict	Slipping	Sometimes considered	In the background	Serious	Serious	Central	Always present
FAMILIAR WITH CURRENT ISP	YES	NO	NO	YES	YES	NO	YES	YES	YES	YES
IS IN DAILY WORK	YES	NO	YES	YES	YES	YES	YES	YES	YES	NO
MAIN REASON FOR COMPLYING	Sense of duty	Fear of risks	Fear of dishonour	Organization's reputation	Respect towards rules	Fear of dishonour	Fear of risks	Conscientiousness	Sense of duty	Sense of duty
ISO 27001 CERTIFICATION FEELS NECESSARY	YES	YES/NO	YES/NO	YES	YES	YES	NO	YES/NO	YES	YES

TABLE 3. Summary of first interview round's general findings

PERCEPTION OF ORGANIZATION'S APPROACH TO INFORMATION SECURITY

Interviewees were asked how they would describe their organization's security culture. According to Theory of Planned Behaviour the organization's general attitude towards information security and compliance could affect the employees' intentions to comply and behave securely. That is why the organization should encourage their employees to act securely by the means of information security policies. The table 3 shows different perceptions of the Securitym 's information security culture. The interviewees were asked to describe their organization's approach to information security. Most of the people answered with an adjective and then started to describe it in more detail. The most common adjective from the answer was chosen to describe their general perception of the organization's security culture.

The results show that some interviewees are describing the approach with similar adjectives but there are a few discords. This can be explained with the different work assignments and different parts the interviewees get to see in the organization. Everyone might also have their own different standard about serious or easy approach to information security.

When the interviewees' answers are examined more closely, 5 of the people described the organization approach to information security as serious or strict. All the interviewees who described the security culture as strict or serious added that sometimes things are slipping out of hand or there are things that could be improved. Two of the interviewees said that in the daily basis information security is a central thing or always present. Three of the interviewees described IS to be slipping, only sometimes considered and it being mostly in the background. Interviewee 8 summarises:

> "The security is taken seriously through information security and software development. Sometimes the practices are shifty, and the execution might vary." (Interviewee 8)

Interviewee 4 reflected that there has been a lot of talk of information security, but security tends to be forgotten in the daily work:

> " It (security) is discussed a lot more than something actually being done to it. At some point we had a lot of different practices but after some time we always tend to slip from them." (Interviewee 4)

These comments show that the information security is emphasized in the organization but sometimes the practices change, or the practices are forgotten in daily work. Other interviewee's answers have similarities. Many of the interviewees mentioned that the security intentions are serious but in the daily work the practices and processes do not function, or they are not on the top of employees' minds. This describes the phenomenon where policies are written and implemented but they are not fully present in the employee's daily tasks.

FAMILIARITY WITH CURRENT INFORMATION SECURITY POLICIES

After describing the overall security culture, interviewees were asked to evaluate their familiarity with the current information security policies. Securitym had their own organizational information security policy which everyone in the organization was following. In addition, the target unit had their own secure software development policy. Interviewees were asked if they were familiar with these policies and how well they knew the security policies' contents.

Seven of the interviewees answered that they are familiar with the current information security policies and three of the interviewees admitted that they are not so familiar with the policies. Some of the interviewees said that they have read these policies through, but some admitted that they have not read the policies. Some of the interviewees mentioned that in the introduction period the IS policies are present but after that they are slowly forgotten.

> “I haven't read the policies through. I would be lying if I claimed to. I have been browsing them sometimes, but not in a familiarizing way. If something needs to be clarified, I check it out from the policy, but I'm not familiar with it on my own initiative.” (Interviewee 6)

Interestingly interviewees 2 and 3 who said that the organization’s approach to information security is strict or serious, were not familiar with the current policies. Interviewee 2 describes their familiarity in a following way:

> “I cannot say that I am very familiar with the information security policies. In a way, basic information has been distributed about what the policies contain and how they affect your own work. I know through common sense what to talk about, where to talk, what to do and what I absolutely should not do.” (Interviewee 2)

Two other interviewees also mentioned common sense when discussing information security policy familiarity. The interviewees argued that if you use common sense, you will not do anything majorly wrong. Common sense might be a good addition to the security culture, but common sense does not include in example information security management’s judgement or risk management.

INFORMATION SECURITY IN DAILY WORK

Thirdly, interviewees were asked if and how the information security policies are present in their daily work. Eight persons answered that the information security policies are present in their daily work and two persons felt like it is not present.

When observing the answers more in detail the observation of information security policies affecting their daily work varied. Some interviewees described how the IS policies affect their daily work tasks:

> “The information security policies appear in my daily tasks, like when asking for a permission to install new software or working remotely.” (Interviewee 1)

Some went more into a detail describing how the information security policies change their daily work. Interviewee 3 described how the policies are slowing down their daily work. Interviewee 3 then added that IS policies are necessary and just an essential part of the IT industry:

> “Yes, those security policies appear in my daily work but in a way that they stiffen and slow down my work. It could be

> faster to work without the policies, but then again if they were not present, that would be a bad thing for the organization. I understand that they (security policies) just belong to the job description when one is working in the IT industry." (Interviewee 3)

On the other hand, two employees felt like the information security policies are not present in daily work. Both interviewees said that the policies are not present in their daily work, but they are affecting everything in the background, for example, access control, communication, and data processing. Interviewees recognize parts where it is present but do not feel like it personally affects their work:

> "Security policies are not an instruction for our daily work that would be reviewed all the time. It is more under the surface." (Interviewee 10)

MAIN MOTIVATOR FOR COMPLYING WITH ISP

All the interviewees were asked what motivates them to adhere to their organization's security policies. This question was asked to find out the motivators that affect the employees' security behaviour. Three of the interviewees described a sense of duty towards their employer and their customers. Two of the interviewees described being aware and fearing the possible risks. Two other interviewees were worried about losing their face. Three other interviewees were complying the security policies because one did not want to risk organization's reputation. One of interviewees described respect towards rules, and one felt conscientiousness.

Sense of duty was the most common answer and it portrayed other interviewee's answers too. The interviewees that answered their main motivator to be sense of duty, described the responsibilities towards their employer or customers. Interviewee 9 described it more in detail adding that information security is individual's duty in the workplace but also in their free time.

> "Today, security is an important issue anyway and cyberattacks are coming from everywhere. It is the duty of the individual to act in a sensible way. In addition, we are responsible for our customers and it is our job to operate safely." (Interviewee 9)

At least the fear of risks could be linked to the Rational Choice Theory which explains IS compliance as employees safe computing behaviour is a rational choice based on the perceived usefulness of the safe behaviour and the possible consequences of not behaving safely. On the other hand, Protection Motivation theory can be used to describe how the employees might follow the information security policies because of the perceived severity of a threatening scenario. This is visible with the employees who said that they are complying with the security policies because of the possible consequences of not complying. Interviewee 7 gave a straightforward answer:

> "Failure to comply policies can lead to serious problems and troubles. That is why I prefer doing things with thought." (Interviewee 7)

PERCEPTION OF ISO 27001 CERTIFICATION'S NECESSITY

After discussing the security culture and information security compliance, the interviewees were asked what they think about the ISO 27001 certification and if it is necessary for their unit. Six of the interviewees felt that ISO 27001 is necessary for their unit. Three of the interviewees were torn between it being necessary or needless. One of the interviewees felt like it might not be necessary to get the ISO 27001 certification.

All the interviewees who felt that ISO 27001 certification is necessary, mentioned its marketing advantage. They described how ISO 27001 is essential when marketing their services or trying to win a contract. As they are doing security, the standard will prove that to the outsiders too. Couple of the interviewees who thought that the certification is necessary mentioned that it will make the processes clearer and give better structure to the practices they have. On the other hand, the interviewees who perceive the standard necessary, had some doubts about it. The main concern was that it is going to make the practices stiffer, slow down the workflow and increase haste. Interviewee 6 described all these viewpoints that many of the other employees had:

> "ISO 27001 standard will bring more bureaucracy. On the other hand, it makes things more systematic and consistent. It ensures that we are following security requirements and we can trust what we are doing more. Even if it brings a lot of rigidity, we must be able to see the positive input. It is not only necessary, it is inevitable. … Our mother company is selling its services as a one unit, so we have to be certified too to contribute to the marketing and sales." (Interviewee 6)

Three of the interviewees did not give a straight answer about the necessity of ISO 27001 certification. All the three interviewees described how they think that the certification will not affect what they do or not raise the standard of their work. On the other hand, they felt that the customers might demand the certification and that is where the necessity might come in. Two of these interviewees were hopeful that it would make the processes clearer, but they were also afraid that it will make their work stiffer. Interviewee 2 described how the ISO 27001 implementation process has not yet changed anything in his or her work and he or she believes that it will not affect their work. After that the interviewee mentions that you cannot even work with some customers without the ISO 27001 certificate.

> "ISO 27001 certification probably doesn't affect what we do. No changes have yet been made that would improve our performance. But in the customer interface I would say that the certification is almost vital. There it is directly stated that the certificate should exist, or you should not even come to knock on the customer's door. You are not good at security if you do not have a certificate. On the other hand, it can serve as a reminder to employees not to loosen up." (Interviewee 2)

One of the interviewees, interviewee 7, argued that he or she cannot judge if the ISO 27001 certification is necessary for the organization or not. Interviewee 7 reckoned that the certification will not increase their work quality and it will slow things down. On the other hand, the interviewee guessed possible positive aspects too. They mentioned that it might increase the sales and ensure more frequent necessary training for the employees.

> "I can't judge if a certificate is necessary for our organization is not. Probably not. The quality of work will probably not increase. If it increases the sales, then its benefits should come through the sales. All in all, the certificate slows things down. Hopefully, it will pay itself back so that there will be less problems that would advance. The certificate might ensure that everyone has received the necessary training and that the training is run through more regularly. If that is the case, there might be at least one positive aspect to it." (Interviewee 7)

Overall, nine out of ten interviewees felt that ISO 27001 certification is necessary at least in some way. The positive aspects that were described were mostly linked to marketing, competitive advantage and process and practice clarification. Some were worried about the bureaucracy it might bring. In addition, some were afraid that it will make their work stiffer and processes slower. Rational choice theory argued that people aim to maximize their personal benefits while minimizing their costs. Thus, if the processes become more stiffer, the policies might fade into the background again.

5.1.3 After ISO 27001 implementation

The state of the security culture and attitudes were studied to give a context and a content to the different stages of the research. The state before ISO 27001 implementation reflected the first stage of the process, the time between the interview rounds reflected the second stage, and the state after ISO 27001 implementation and auditing reflects the third stage of the process. To examine the general perceptions and attitudes towards information security, information security policy compliance and ISO 27001 implementation, the interviewees were asked questions related to their experiences and attitudes. The questions were based on the first interview round to see if there have been any changes related to the studied information security aspects. In table X the general results are presented in a simplified form. These themes were discussed using the following questions:

1. How would you describe your organization's approach to information security?
2. How familiar are you with current security policy?
3. How security policies are present in your daily work?
4. What motivates you to adhere to your organization's security policies?
5. Do you feel that ISO / IEC 27001 standard certification is necessary? What did it bring to your daily work? How did it affect your daily work?

The answers are categorized in the following table to give a quick overview of the general findings of the second interview round:

	I1	**I2**	**I3**	**I4**	**I5**	**I6**	**I7**	**I8**	**I9**	**I10**
MAIN IMPRESSION DESCRIBING INFORMATION SECURITY CULTURE	Considered	Serious	Uncontrolled	Considered	Serious	Serious	Serious	Considered	Serious	Serious
FAMILIAR WITH CURRENT ISP	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO
IS IN DAILY WORK	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
MAIN REASON FOR COMPLYING	Organizational culture	Sense of duty	Sense of duty	Sense of duty	Sense of duty	Fear of risks	Fear of dishonour	Conscientiousness	Sense of duty	Trust
ISO 27001 CERTIFICATION FEELS NECESSARY	YES	YES	YES	YES	YES	YES	- (cannot state yet)	YES	YES	YES

TABLE 4. Summary of second interview round's general findings

PERCEPTION OF ORGANIZATION'S APPROACH TO INFORMATION SECURITY

First, the interviewees were asked how they would describe their organization's security culture. Table 4 shows different perceptions of the target organization's information security culture. The interviewees were asked to describe their organization's approach to information security. Most of the people answered with an adjective and then started to describe it in more detail. The most common weighted adjective from the answer was chosen to describe their general perception of the organization's security culture.

When the interviewees' answers are examined more closely, 6 of the people described the organization approach to information security as serious. Three of the interviewees described information security in their organization to be considered. This seemed to mean that it is something that is kept in mind when doing different projects and tasks. One of the interviewees described organization's information security being uncontrolled.

Many of the interviewees who said the information security is taken seriously, added that it has increased during the ISO 27001 implementation process. It seems that the interviewees had different visions of a good level of information security. Interviewee 7 describes the situation in depth:

> " Information security is taken very seriously here. Nowadays even more time is spent on it. It is such a balancing act. It is impossible to have a completely secure environment, so you have to think about how you will create something other than information security in the process while doing your work. Information security tries to balance with usability and schedules. Some people try to pursuit perfection around information security. It is frustrating that some people think you have to take security as far as possible, even if you should just execute processes that make sense in the real world." (Interviewee 7)

Interviewee 3 who described the information security to be uncontrolled, described the information security in their organization in a following way:

> " It is allowed for us to work pretty freely in our organization. I think some things could be handled with more care easily. For example, management of passwords and certificates is executed poorly. Now they are stored who knows where." (Interviewee 3)

Between the two interview rounds interviewees' description of their organization's attitude towards information security got more favourable. In the first interview round people had to think more about how the information security is perceived and three of the interviewees gave the impression that the information security is not in a good level. In the second interview round, only one interviewee described it negatively. It seems that the approach to information security has become stricter during the ISO 27001 implementation. This can be seen as a natural process since ISO 27001 forces the organization to consider their own information security processes, document them and also prove them to the auditing party.

FAMILIARITY WITH CURRENT INFORMATION SECURITY POLICIES

After describing the overall security culture, the interviewees were asked to evaluate their familiarity with the current information security policies after the ISO 27001 implementation. Securitym still had their own organizational information security policy which everyone in the organization was following. In addition, the target unit had their own secure software development policy that was projected from the ISO 27001 standard. The interviewees were asked if they were familiar with these policies and how well they knew the security policies' contents.

Nine of the interviewees answered that they feel that they are familiar with the current information security policies and only one of the interviewees admitted that they are not so familiar with the policies. Some of the interviewees stated that they still had not read the policies through but that the policies were more in discussion and became more familiar during the ISO 27001 process. Interviewee 5 described their familiarity with the information security policies in a following way:

> "Well, let us say that on a scale of from 1 to 3, I would describe my familiarity as a 2. I have the basic skills, but I am not an expert with the policies. Thus, my basic competence includes what is good information security practices in the daily work and how our work is done in a secure way and how to act if an emergency arises. E.g. If a virus infects my computer, I know who to call to. We had an ISO security audit in the spring, so there was quite a lot of communication on this subject. There was a reminder of the security policies from the organization and at least our familiarity with the policies has not gotten any worse now." (Interviewee 5)

Same themes were present in other interviewee's answers as well. Interviewees described how they have a basic knowledge of the security policies and that they have been remined of the policies during the standard implementation process. Compared to the first interview round, more people felt like they are familiar with the information security policies: in the first interview round 7 interviewees felt like they are familiar with the information security policies and in the second round 9 interviewees felt like they are familiar with the policies. Overall, people seemed to have more confidence with their familiarity with the IS policies and the knowledge related to information security.

INFORMATION SECURITY IN DAILY WORK

Thirdly, interviewees were asked if and how the information security policies are present in their daily work. In the first interview round only eight interviewees felt that information security policies are present in their daily work. After ISO 27001 implementation and auditing, all the interviewees answered that the information security policies are present in their daily work.

Interviewee 3 described how the information security policies are present in everything the target unit is doing in a following way:

> "Basically, information security is heavily involved when designing new software here. It takes a lot of time and energy to think about how you do something securely. Information security regulations are considered in the design process. Security can affect the whole software architecture. From the application development side, we have security reviews and there have been discussions of various lists like OWASP and SANS TOP 25 which tell you what security aspects to consider when doing software development. We consider security to minimize the possibility of damage. But in the end people make mistakes, but we are doing our best to avoid them. Everyone has a responsibility to do their work securely. In example, we don't have a security architect here since everyone is accountable for security." (Interviewee 3)

Interviewee 3's answer shows a strong information security culture that is present in the whole target unit. Interviewee 3 describes how they do not have a security architect and how everyone has responsibility to work in a secure way and consider information security. Theory of Planned Behaviour underlines the individual's intention to perform a behaviour which affects the actual behaviour. In addition, the organization's general attitude towards information security and compliance could affect the employees' intentions to comply and behave securely. Interviewee 3's answer emphasizes the intentions and culture of the employees who feel like the information security is a shared responsibility. This kind of shared responsibility and a strong team spirit was emphasized in the second interview round.

Interviewee 10 stated in the first interview round that security policies are not an instruction for their daily work. In the second interview round interviewee 10's perception had changed, and they described the information security in their daily work in a following way:

> "We are still in same company and the same requirements are valid. I wonder whether things are now actually better in a target unit's product development than elsewhere in this whole organization. It feels like things are not involved in everyday work everywhere here, but the target unit involves the policies

> in daily work. Interestingly, the other organization has been audited for a long time, but you don't see those regulations as present elsewhere." (Interviewee 10)

In addition to the change in interviewee's perception of information security policies in daily work, the interviewee also stated that the information security policies might be more present in the target unit's daily tasks than in other parts of the organization. This is an interesting perspective since other parts of the organization had been audited before. This view could be explained with the fact that the target unit had to tackle the ISO 27001 requirements in the software development's context themselves. No one gave the straight answers to them directly and they had to figure out the new changes themselves. This might reflect to the daily work in a way where the ISO 27001 requirements are fitted to the employee's work and not vice versa. There might be a possibility that employees consider the information security policies more in their daily work if they have been involved in the development process.

MAIN MOTIVATOR FOR COMPLYING WITH ISP

All the interviewees were asked what motivates them to adhere to their organization's security policies. This question was asked to find out if the motivators that affect the employees' security behaviour have changed after the ISO 27001 implementation. Five of the interviewees named their main motivator to be sense of duty. Individual answers considered organizational culture, fear of risks, fear of dishonour, trust, and conscientiousness. The themes discussed were similar to the first interview round, but the discussion gravitated towards positive motivators instead of fear being the motivator.

The interviewees that answered their main motivator to be sense of duty, described the responsibilities towards their organization or customers. Many of the interviewees described how it is their duty to comply with information security policies and work securely. Interviewee 2 described this sense of duty coming for their inner motivation:

> "Compliance is about duty and professional pride. I think that compliance comes from my intrinsic motivation because I want to do my job well and produce quality work. Those are the biggest factors I can name. … the most important thing is you can trust what you are doing is right and develop yourself in that." (Interviewee 2)

Like Zinatullin (2016, p. 89) described, intrinsic motivation comes from within the individual and this kind of motivation usually leads to behaviour which is rewarding for the person himself. Instinct motivation factors could be enjoyment, interest and meaning. Like discussed in literature review before, Jai-Yeol (2011) found out that security policy compliance approaches relating to the intrinsic motivation paradigm led to a significant increase in compliant employee behaviour over approaches that handled the extrinsic motivation model. This decrease of extrinsic motivation related to fear and increase in intrinsic motivation like sense of duty could have effect on the employees' ISP compliance in the target unit as well.

As other themes remained the same, trust was the only main motivator that was not brought up in the first interview round's answers. Interviewee 10 brought up trust for their own work as a main motivator for ISP compliance in a following answer:

> "The main motivator for me is trust. What matters most for my compliance is seeing why things are done and being confident that it will bring security with it. It is important that processes have actual value, and we do not just follow the policies because there is a certificate that tells us to. I also see it as a personal matter that I can trust what we are doing." (Interviewee 10)

It seems that for interviewee 10 trust towards their work and security value in processes motivate her in complying with the ISPs. Surprisingly, the literature reviewed did not handle trust as something that might affect the employee's ISP compliance.

Supposedly, after the ISO 27001 implementation more people felt like the information security compliance is their duty and they feel responsibility towards their organization and customers. Fear of risks or dishonour diminished by two interviewees during the interviews. Overall, the conversations' tone changed from "what could happen if something to wrong" to "what we need to do so things do not go wrong?". There might be a change in information security culture, but deductions should not be made after only 3 months after implementation.

PERCEPTION OF ISO 27001 CERTIFICATION'S NECESSITY

After discussing the security culture and information security compliance, interviewees were asked what they think about the ISO 27001 certification and if it is was necessary for their unit as a target unit. Nine of the interviewees felt that ISO 27001 was necessary for their unit. One of the interviewees felt that the question cannot be answered before a longer time has passed and the necessity can be more properly evaluated.

As mentioned, almost every interviewee felt that the ISO 27001 certification was necessary for their unit. The main themes that interviewees brought up related to the necessity were clearly documented processes, more specifically identified and increased information security, and marketing advantage. Interviewee 6 discussed ISO 27001 certificate's necessity to organizational culture, processes, and marketing in a following way:

> "Perhaps that certificate reinforced to the organization culture that information security is really built into our work. It reminded us that things need to be done in a right way and that things are done in a way we claim to others we are doing them. I think the parent company has had the certificate for a long

> time, so we still have things to develop and they need to include us more. Now the certificate made clear to us that information security is not a matter of play and we are really part of this organization and we also must act according to the certificate. We must have that certification and if we do not have it, it would be a disadvantage for us. So, it is absolutely necessary. Now there is no need to prove to others in any other way that we are a secure organization." (Interviewee 6)

The interviewee who said that the necessity cannot be assessed yet, explained their answer in a following way:

> "ISO 20071 made things harder for us since the time spent on processes increased. It is yet impossible to say whether it will pay back all the time spent. You never know if you have noticed all aspects related to information security. At least, the standard reduces the risk of vulnerabilities, but it does not eliminate them. I cannot yet state if it is too heavy to process or if it becomes more convenient. I don't know how it works yet." (Interviewee 7)

Overall, it seems that the perceptions of ISO 27001 certification's necessity changed towards more positive after the ISO 27001 auditing since the number of interviewees who thought the certification was necessary increased from six employees to nine employees. The themes behind the necessity evaluations stayed similar.

5.1.4 Experiences of ISO 27001 standard implementation in a software development environment

The ISO 27001 standard implementation affected the whole target unit. Some of the interviewees were part of the standard implementation team and some of them were just bystanders. In any case, the standard implementation affected everyone's daily work since it changed the processes and practices related to information security. To examine how the ISO 27001 standard fits into a software development environment, the interviewees were asked "How did you experience the ISO 27001 standard's implementation in a software development environment?". Many of the interviewees brought up topics related to the standard's suitability, management's support and information sharing throughout the process. Some of the interviewees thought that the ISO 27001 is suitable for software development if the requirements can be interpreted unambiguously. On the other hand, some of the interviewees said that the ISO 27001 is too rigid to software development and it requires a lot of work to get the standard match with software development processes. Themes about managements support and effective communication were also criticised by some of the interviewees.

STANDARD'S SUITABILITY FOR SOFTWARE DEVELOPMENT

Interviewee 10 describes their experience of the ISO 27001 standard's suitability for software development in a following way:

> "ISO 27001 bends to software development stiffly because it is not written from a software development perspective. It is apparently written more from a system perspective. It seems that it is assumed that an outsourced information system is implemented in the organization and that system is then used and maintained. This perspective will make it easier to understand the requirements of the standard in the information system context. But we make systems ourselves that are used and sold by our own organization. Therefore, there are so many angles of entry to the standard, and they were really hard to interpret. It terribly requires an interpretation of that software development perspective, at least for the first timers. There were individual requirements that were always stumbled upon, which started a long discussion every single time. Interpreting requirements was difficult when the context was different from what is done in software development. I can say that ISO 27001's requirements were not one with software development's requirements. Scope changed every time the standard was discussed. It was a challenging experience." (Interviewee 10)

Interviewee 10 felt like the ISO 27001 is written from a perspective that handles organizations that buy outsourced information systems rather that develop the systems themselves. Interviewee 10 described their experience as challenging. Interviewee 7 describes their experience as challenging as well but adds that there are different paths to reach the same ending point since organizations and even units inside them can work very differently:

> "We got the ISO 27001 standard somehow bent to software development, but it was a challenge. It does not make software development very agile, but I guess it increases information security. It remains to be seen. Very similar problems can arise for other software companies. But it depends on the people around the implementation. Classically, you can limit the scope of a standard, whether it is just a function of a unit or an entire company. Limiting the scope already does wonders. The experience can change if you change many processes or if you just pretend that you are changing a lot of processes. The third thing is whether to overinterpret things. There are a huge number of things you can do, but you do not have to do everything. We needed to identify many things we do and tell that we have been identified these, but we are not going to change

> this and then tell the auditor why. You can still pass the auditing even if you do not handle every aspect. ISO 27001 certified companies or parts of it can be really far apart in how they actually do things. We needed to be able to show that security is being tested better, so we told that we would rely on SANS and OWASP vulnerability lists, but we would not have been forced to do so. There are many paths to the same point when it comes to standards." (Interviewee 7)

Biggest issue with ISO 27001 standard's suitability in software development seemed to be the diverse nature of the projects that the target unit handles. ISO 27001 fits to projects that produce products inside the target unit for universal markets. But if the project is an order from customer, the project composes of things that the customer requires. For example, if the customer does not want to pay for vulnerability testing, vulnerability tests are not made, and the information security might be disregarded. This is a once again a conflict between ISO 27001 requirements and real working environment. Interviewee 3 describes their experience of ISO 27001 standard's suitability in a following way:

> "I would say that the ISO 270001 standard bends to software development. We noticed that it fits well to product development where we develop products that we mostly sell. But for example, we have a small team that focuses on doing commissions directly to customers and then it is only about what the customer is willing to pay for. For example, if a customer says that they do not have enough money for security testing, we can not to say that we are ISO 27001 certified and the customer is forced to do information security testing and they must pay for it. We tried to avoid this dilemma in audit by describing our product development and customers projects separately. But then the audit only went through the product development side and the work we had done seemed to be pointless." (Interviewee 3)

MANAGEMENT'S SUPPORT

Interviewee 3 continued about their experience about the ISO 27001's suitability and what could have been done better. They described how Securitym could have hired a consultant to help the target unit or at least give better guidance related to the standard's scope:

> "Well, in my experience I think the biggest thing that could have been done differently related to ISO 27001's suitability would have been hiring a consultant tell us what to do. It would have saved us time and money and a lot of energy. That is perhaps the biggest thing I would have changed. There are professionals who have done standard implementation, so they

> could have been a huge advantage to us. I wish a consultant could have made it clearer which things really belong to the standard's scope. Or maybe the parent company could have told us that. When we asked our organization about the scope of customer projects, they told us to focus on them in the documentation, but the auditor was not interested in them at all in the auditing event. That was just a waste of time." (Interviewee 3)

Interviewee 3 hoped that the target company's management would have guided the target unit more in the implementation process or supported them financially and hired a consultant to help them. Management's support in underlined in many successful projects and it seems to apply to this implementation project as well. Interviewee 6 also brings up their expectations of Securitym management's support in the implementation:

> "My experience was that our roles could have been even clearer. In a way, our parent company just expected that this target unit has always been diligent and once again it was trusted that we will take care of this independently. I would have craved for more guidance and leadership from the parent company's management. It feels like we were just left alone." (Interviewee 6)

Top management's support has been found out to be a glue between the leadership and project success which can strengthen or weaken the relations. Unfortunately, in practical terms top management cannot take care of every project in the organization. (Khan, Iqbal and Long, 2014). This seem to be the case in this research since Securitym was asked to step in and help with the implementation, but the target unit did not find that the guidance offered was enough.

COMMUNICATION

An interesting finding was made related to the communication aspect of the implementation process. Like in Hsu's study, where the employees and the managerial level felt differently about the success and communication of the standard implementation, during this study there were similar themes observed. All the managers that were interviewed were pleased with the success of communication and the amount information that was offered during the implementation process. Interviewee 9 describes this in a following way:

> "Employees were informed of the certification through the intranet and the final report was also available. The team meetings covered the intranet news and the supervisor's meetings covered these issues and also the final outcome. Our communication in intranet works well. After the auditing, there was information available in our instant message application as

> well. Communication worked really well during the whole implementation." (Interviewee 9)

On the other hand, some of the employees felt that there has been a lack of communication and they have not been sure about the different stages of the implementation process and what was required from them. Especially the employees who were not part of the implementation team felt that there has not been a lot of communication about the ISO 27001 standard. Interviewee 4 describes:

> "Quite little information was provided to the external groups outside the implementation team. We were told that implementation is in progress and this is the deadline. Information was not widely shared and there was little communication outside the implementation team. Maybe they were too busy to communicate. I would have loved to hear more often about what the status was and who was involved. Almost the whole process would have needed better communication. More information about the whole ISO 27001 structure and about the roles that other employees have." (Interviewee 4)

Interviewee 1 adds their perspective:

> "There was no training in the standard. Nor have there been any decent information sessions. The message came only that the audit went through. Team meetings reviewed what practices will be and what vulnerability listings need to be reviewed and what they mean." (Interviewee 1)

It seems that the managers felt that the communication was appropriate, but the information did not reach the employees that were not part of the implementation team. Similar phenomenon was present in Hsu's (2009) study where she highlighted possible differences between standard implementation experiences between managers and employees. Hsu's study proved how important effective communication is in an implementation process. Hsu observed a security certification implementation process is an organization and compared management's and employees' impressions of this process. During the process of implementing information systems security certification management's intentions were good but the managers did not really have the time to communicate the whole process to the employees.

Overall, the ISO 27001 implementation process seemed to take a lot of time and energy from the interviewees. Some of the interviewees hoped that top management support and communication would have been better. However, every interviewee was pleased with the auditing results since they felt they could affect new processes themselves and, in the end, they got the ISO 27001 certification. Interviewee 5 describes their positive experience of the ISO 27001 standard's implementation in a following way:

> ”My experience with the standard was good, no contradictions come to mind. … In a way, the standard forced us internally to observe processes and practices. It made us really reflect what we could improve. Otherwise we would probably never evaluate these information security processes.” (Interviewee 5)

5.2 Conflicts between ISO 27001 standard requirements and daily work

As the context of the organizational changes have been mapped, the discussion with the interviewees grew deeper and new aspects were discovered. One interview question about ISO 27001 disciplinary requirements sparked up a versatile conversation since the interviewees felt like disciplinary measures do not fit into a Finnish organization. In addition, interviewees brought up a huge problem related to their code reviewing process which affects the information security aspect, but which ISO 27001 does not offer a guidance to.

In this subchapter the research questions ”What kind of conflicts might appear between ISO / IEC 27001 standard requirements and day-to-day work?” and ”How the target unit resolves the conflicts between ISO / IEC 27001 standard requirements and day-to-day work?” are discussed. These conflicts describe well how standards do not invariably reflect the practical world.

5.2.1 Description of emerged conflicts

The biggest issue that came up in the interviewee process was ISO 27001 not fully suiting a software development environment. The employees that were handling the implementation and auditing, mentioned how they had to interpret ISO 27001 standard’s requirements a lot. The requirements did not straightforwardly transfer to their software development environment and this caused conflicts between the practical world and standard documentation, and even between the employees working with the implementation.

Two of the biggest conflicts the employees working with ISO 27001 implementation faced were with the code reviewing process and disciplinary measures. This can be concretized as duality, an instance of opposition between two concepts of something. In practice, code reviewing processes needed to be organized to increase information security and overall security of the software, but ISO 27001 does not imply any practical requirements or processes related to the software development’s information security. Hence the standard does not state the practical needs. On the other hand, ISO 27001 requirements include disciplinary measures which need to be documented. The interviewees argued that disciplinary measures do not fit into Finnish organization. Therefore, the standard also creates conflict between practice and its requirements. Thus, the duality forms.

CODE REVIEWING

Code reviewing was the first issue that came up during the first round of interviews. In general, code review is a software quality assurance activity. Baum, Liskin, Niklas and Schneider (2016) give two different definitions of code review. The first definition states that in code review the main checking is done by one or several employees, at least one of the employees is not the employee who wrote the code, the checking is made by viewing the source code and it is performed after the implementation or as an interruption of implementation. The second definition states that code review is codified in the development process of the development team. Every time a unit of work as in part of a code is seen as ready for review, all changes from the previous unit are assessed. If the review is seen as necessary, the work unit waits for the reviewers to evaluate the code.

ISO 27001 standard's Annex A.14.2 is about security in development and support processes. The objective is to make sure that information security is designed and implemented within the development lifecycle of information systems. ISO 27001 standard's Annex A.14.2.1 focuses on Secure Development Policy. It requires that rules for the development of software and systems should be established and applied to the internal development of the organization. Secure development policies are meant to ensure that development environments are secure and system changes encourage the use of secure coding and development practices.

Six out of ten interviewees brought up the issues of their organization's code reviewing process during the first interview round. These interviewees told that there has been a code reviewing process, but it was just too ponderous to follow. It was abandoned gradually and now the target unit has no code reviewing process at all. This situation can be linked to the Rational Choice Theory which argues that employees safe computing behaviour is a rational choice based on the perceived usefulness of the safe behaviour and the possible consequences of not behaving safely. If the behaviour is too troublesome, it might be rejected even if its results might be useful to the security. Interviewee 3 described their situation in a following way:

> "As we are doing software the code reviewing process could be better. It could be handled in a way where you are forced to go through the reviewing process. Now the organization just trusts that someone will go through the code. The code reviewing usually is eventually done but there is still an opportunity that you forget it, or it just gets ignored. This ISO project has tried to improve those processes." (Interviewee 3)

Interviewee 7 argues that there is no systematicity in the code reviewing process. Interviewee thinks that the new process will add more burden to the employees like the old code reviewing process but is still hopeful that it will reduce the incidents customers report:

> "We had code reviewing processes before, but it was so burdensome it became voluntary. Now the code reviewing process starts if a developer asks someone to review their code and the reviewing process might start when someone has the time. There is no systematicity. Because of ISO 27001 implementation we will go towards the systematic approach again. Of course, it will burden us since we must find the time to review other's code. It will make everything slower. I hope the new process will cost itself back so there will be less issues coming from the customers' end." (Interviewee 7).

Interviewee 7 continues describing the ISO 27001 implementation process and the documentation that must be done for auditing. Interviewee describes it as heavy and time-consuming. The main issue seems to be different interpretations of the ISO 27001 requirements and ISO 27001 not fitting to their working environment:

> "This whole ISO 27001 implementation is insanely heavy. It feels like you are more than half the time guessing what these requirements mean in practice. ISO 27001 specifications are so circularly written that there can be no concreteness about what needs to be done correctly for example in code reviewing. Those different interpretations go all over the place and we go through the same things repeatedly. This is an energy consuming task. I wish we had someone who could explain the standard from a software development perspective." (Interviewee 7)

Over half of the interviewees brought up their wishes about the new and better code reviewing processes to improve their software development. It seems that new reviewing processes are highly needed but ISO 27001 standard does not give a clear explanation of required code reviewing processes. This caused confusion and distress among five of the interviewees.

DISCIPLINARY MEASURES

In addition to the conflict between the daily work and the lack of specification in the ISO 27001 standard requirements, an interesting finding was made during the interviews. Since Deterrence Theory is broadly studied in information security research and ISO 27001 requires disciplinary measures, a question about disciplinary measures was presented. The interviewees were asked a question "In what situations should disciplinary measures be used if any part of the security policy has been disregarded or has not been literally complied with? What do you think of disciplinary action in these situations?". All the interviewees had a negative impression of disciplinary measures overall, but they were able to name situations where these measures would be appropriate. The answers were unanimous as indicated in a following table:

	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10
FINDS DISCIPLINARY MEASURES BENEFICAL	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO

TABLE 5. Summary of employees' attitude towards disciplinary measures' usefulness

ISO 27001 states disciplinary measures in Annex A.7.2.3. as disciplinary process. Usually disciplinary process can take different forms from reprimand, verbal or written warning, decrease in monthly salary, all the way to dismissing employment. ISO 27001 states that there needs to be a documented disciplinary process for security breaches which must be communicated to employees clearly.

During the interviews it became clear that disciplinary measures do not motivate employees who work as specialists. When the interviewees were asked in what situations disciplinary measures are acceptable, they described mostly situations in which the employee would break Finnish laws among with the organization's information security policy. In less serious cases the dominant opinion was that disciplinary measures are unnecessary and even demotivating. Interviewee 4 described their attitude towards disciplinary measures in a following way:

> "Disciplinary measures would affect us in a way where we would not dare to do our work in the same way anymore or take responsibility of things. It would make my view of the employer very negative and if we would be threatened with disciplinary measures, I might even consider cancelling my contract in that situation." (Interviewee 4)

Similar effect was found in the literature review in Zinatullin's study in 2016. Zinatullin (2016) proposed that the solution to security compliance would be the raised costs or lowered benefits of non-compliance. For example, employees could be punished. On the other hand, he argued that this could tarnish the reputation of the security function if the employees become too scared to do their day-to-day tasks because of the potential punishment.

Even the managers did not find disciplinary measures natural. One of the managers argued that there are reasons behind non-compliant behaviour and a manager should be able to notice warning signs before a security breach. All the managers considered that disciplinary measures would lower the work morale. Interviewee 6 described:

> "It is not natural for me to rely on disciplinary actions. I always try to think of something else first. On the other hand, as a supervisor I think there is always something else behind

> the non-compliance that I should have been able to detect. Good supervisor can notice that this person is not going in the right direction. I do not think that the punishment is a good way to handle these situations. Not the best motivational tool. It even weakens the work atmosphere." (Interviewee 6)

Interviewee 10 asserts:

> "Disciplinary measures would extremely negatively affect people. We are in the creative field and have a smart and educated team. If the leading would happen through communicating punishments, the negativity of it would spread to the whole working environment." (Interviewee 10)

Target unit's organizational security culture seems to be strong according to Interviewee 5's observations. Interviewee 5 described how their peer-to-peer mischief works better than disciplinary processes. Interviewee described their work community's security behaviour reminding in a following way:

> "When it comes to negligence, training is a way better option than disciplinary measures. If the negligence is repeated, maybe there could be some punishments. I think that our crew's measures are better: if someone leaves their computer unlocked, we do some kinds of mischief to remind them. If someone is not wearing a badge, the person is guided to leave the building." (Interviewee 5)

Based on Theory of Planned behaviour, organization's general attitude towards information security and compliance could affect the employees' intentions to comply and behave securely. If the peer-pressure is present and co-workers use these kinds of friendly reminders of information security policies, the disciplinary measures might seem too strict. Based on the interviews it seems that ISO 27001 disciplinary measures and General Deterrence Theory's teachings does not fit into a Finnish specialist-based software development organization as such.

5.2.2 Resolutions

The target unit faced duality in interpreting ISO 27001 information security management standard. Employees working with the implementation had to find a resolution to the conflicts that emerged between the standard and practical work. In the second interview round, the interviewees were asked how the conflict with the code reviewing were resolved. Secondly, they were asked if they have come upon disciplinary measures during the implementation process or in the auditing. If the interviewees had not heard about the disciplinary measures, they were asked if they know what the consequence of information security policy non-compliance would be, since ISO 27001 standard requires documentation of the disciplinary measures and a clear communication of the measures to the employees.

CODE REVIEWING

In the first interview round, six out of ten interviewees brought up the issues of their organization's code reviewing process. It was clarified that there has been a code reviewing process before the interviews, but it was just too ponderous to follow and it got abandoned. The target unit ended up in a situation where code reviewing was sometimes done but no one was following the code reviewing compliance and if it was sufficient. Interviewees brought up their wishes related to the ISO 27001 standard's impact on code reviewing processes. Interviewees were working with the ISO 27001 documentation brought up the conflict between the ISO 27001 standard's requirement interpretation and real-life demands in the working environment.

In the second interview round the interviewees were asked to describe how the conflict between the ISO 27001 standard requirements and the real-life demands were resolved. In addition, they were asked to describe their current code reviewing processes and their effectiveness. The code reviewing processes had passed the auditing and employees seemed to be more pleased with the new process compared to the old one.

The first question related to the code reviewing process was about the conflicts that appeared between the ISO 27001 standard requirements and real-life demands. Some of the interviewees were not able to describe the conflict resolutions because they were not a part of the implementation team that took care of the implementation and documentation. Interviewees who took part in the implementation process described the conflict resolution in a following way:

> "The code review complies with ISO 27001 standard since the code review requirements advise on which checklists the code should be compared to. I still do not know what ISO 27001 says about code review in detail. An interpretation had to be made about the execution." (Interviewee 2)

> "ISO 27001 does not give an opinion on code reviewing process, but it hints that your processes should rely on some well-known mechanisms. So, then we concluded that it is worth relying on known vulnerability lists. We did not interpret the standard, but rather just speculated it. Apparently, our speculation turned out to be right." (Interviewee 7)

> "ISO 27001 standard did not state how the code reviewing process should be handled but then it did not tell us anything practical anyway. The standard does not seem to comment on how things should be done. You just have to hope your resolution fits the requirements in the end." (Interviewee 10)

All the interviewees who described the conflict resolution, brought up the issues related to interpretability of the ISO 27001 standard's requirements related to code reviewing. Interviewees pointed out that ISO 27001 hints that the code reviewing can rely on some well-known mechanism or vulnerability lists and the implementation team decided to rely on them. The target unit is comparing the code reviewing customs to vulnerability lists like OWASP top 10 which makes the information security aspect of the code more considered.

It seems that the ISO 27001 standard requirements were confusing to the employees who were implementing the standard. The interviewees describe the execution as an interpretation and speculation. The employees were not sure if their guesses were right until the end which referred to the auditing. Two of the interviewees expressed their experience with the interpretation as stressful and tiring.

After the question related to the code reviewing conflict resolution, all the interviewees were asked to describe their current code reviewing processes. All the interviewees were capable to describe the reviewing process and were familiarized with it. The code reviewing is organized in a following way according to interviewee 1:

> "Before ISO 27001 implementation we had to review code that was in different project and it was hard to find time for it. Now we have designated code reviewing pairs who take care of the code reviewing when it is their turn. If I am programming user interface, I will code review other's user interface work. The process is not too heavy, and it has already become a routine for me. We get an automated message from the version control program when we need to review someone's code. If we still forget to do it, our team leader will remind us of it. In addition, people with different kind of experience overview each other's code now so we learn from each other: especially the young programmers can learn from the more experienced ones' code. I think we have learned from our previous mistakes." (Interviewee 1)

> "The systems we already have were used to help with the code review. At least a new code package was made, so it became a confluence report on it. Then every day there is a working couple who take turns reviewing.
> On the day they have their own review shift, they must spend their working time on it and do those reviews. If there are comments, then there is a way for those comments to go back to the developer. In the past, we had a Word document that was hard to come by and it was heavy. No one uses it
> demanded, then no review was made. That is why now those who do that code review got it for themselves
> make it a review process design. Of course, they themselves

> want to do a process that is easy to follow as well. "(Interviewee 10)

Based on the interviewee's descriptions, it seems that the new code reviewing process is more automated and ordinary. The target unit has assigned code reviewing pairs who have their own dedicated turns when they need to review other developer's code. The time that is spent on code reviewing is designated beforehand so the employees have time to review code. An automated message is sent to the dedicated reviewing pair when a code package has been pushed to the revision control. If the reviewing pair do not review the code in time, their team leader will notify them about it. When the code is reviewed, the reviews must check that they have reviewed the code and there is a record made of it.

One aspect related to ISO 27001 standard is that organizations must be able to prove the security measures they have implemented. Before the target unit had no proof even inside their own organization that the code reviews have been carried out. Now the situation has changed as the interviewee 3 describes it:

> "Before we did not have any proof that the code reviewing was carried out. Now we can prove that the code reviewing is done because you have to check off that you have done it and then there is a record left of it." (Interviewee 3)

Overall, the code reviewing process seems to be more structured and it can be proven that code reviewing has been carried out with every new code packet. All the interviewees described the new code reviewing process as a major improvement. On the other hand, they mentioned that is more time consuming and the developers have less dedicated time for programming. Even the interviewees who criticised that the new process is time-consuming, admitted that it increases information security and can pay back the time consumed. ISO 27001 was not straightforward about the execution of code reviewing but the target unit was able to answer the requirements by following known vulnerability lists and mechanisms.

DISCIPLINARY MEASURES

In the first interview round the ISO 27001 standard's disciplinary measures were brought to discussion because Deterrence Theory is broadly studied in theory in information security research. All the interviewees had a negative impression about the disciplinary measures in the first interview round. None of the interviewees had heard of the disciplinary processes during the implementation process before the auditing. This opened a series of questions about the handling of the disciplinary measure documentation demand. The interviewees were asked if they faced disciplinary process documentation during the documentation and implementation process and if not, do they know what the consequence of information security policy non-compliance would be.

When the interviewees asked if they had come upon ISO 27001 disciplinary requirements during the implementation or auditing process, all the interviewees answered that they had not heard of them besides in the first interviews. Even the employees who took part in the auditing did not recognize the required disciplinary measures. Interviewee 7 described the situation in a following way:

> "At least I haven't come upon the documentation nor remember having received any documentation about the disciplinary measures. ... Maybe it is part of the documentation that must be read at the beginning of the employment, but there is no memory left of it. In principle, there may be something in the employment contract bases that if you act against the company, there will be sanctions, but no one will think about them after the first day." (Interviewee 7)

Interviewee 7 suspected that the disciplinary measures might be documented in the instruction materials that are read in the beginning of the employment. It seems that the target unit did not document the disciplinary measures themselves, but Securitym has handled them in an organizational level. After this assumption was confirmed with the Securitym's representative, it was assured that the disciplinary measures were handled in the organizational level by Securitym and that the documentation was available in the organization's internal website.

Since the disciplinary measures should be clearly communicated to the employees in any case according to the ISO 27001 standard, the interviewees were asked if they knew what the disciplinary measures would be if they would not follow the information security policies. It became clear that the employees were not familiar with the disciplinary process documentation nor the possible consequences of non-compliance. Interviewee 5 had not heard about the disciplinary measures at all and described the lack of information in a following way:

> "I have never heard of disciplinary actions. There has not been communication about them that I would have internalized. I could imagine that a supervisor should communicate these measures to us. I have no clue if we would have any sanctions of information security policy violations. If something like that happens, I am going to argue that we have not been told about the consequences!" (Interviewee 5)

It seems that the disciplinary processes have not been communicated at all. Some of the interviewees pondered that their employment could be terminated if they did something as serious in the terms of information security as broke the Finnish law. Interviewee 1 described it in a following way:

> "No one has told me about the disciplinary measures. I do not know what happens if I commit a security breach. At company level, there may have been some talk about fines, but I do not know what else will result from policy violations. If you intentionally do something wrong, then the employment relationship will probably end there." (Interviewee 1)

Overall, it seems that not communicating the sanctions is the resolution even if it is in contradiction with the standard. Securitym has handled the documentation of the processes, but the disciplinary measures and processes are not clearly communicated to every part of the organization. This is not in line with the ISO 27001 standard's requirements. On the other hand, the interviewees argued that the disciplinary measures would be highly demotivational and one interviewee even mentioned that they would leave their employer if disciplinary measures would be normalized. This could force the employer to be in a situation where they must document the disciplinary measures but leave them uncommunicated.

6 DISCUSSION

ISO 27001 information security management standard is one of the most widely implemented information security standards in the world. It can improve organization's information security processes and increase organization's marketing advantage. In this thesis, the literature review was conducted to identify which factors can have affect organization's information security culture and if they are related to information security management standards. Deterrence theory stood out from the literature review since it is widely used in information security research and ISO 27001 standard requires documentation of the disciplinary measures. In the empirical study, the ISO 27001 standard implementation and auditing process was observed from an outsider's point of view. Employees' own perception of the information security culture, ISO 27001 standard related challenges and ISO 27001's suitability to software development were observed through a case study.

The literature review did not answer how ISO 27001 can affect security culture and employee's security behaviour. Therefore, the themes for the interviews were built based on the themes that were missing from the literature review. The goal was to understand this complex phenomenon around ISO 27001 implementation from the employees' perspective in an organization for which information security is crucial. Thus, in this chapter the results of the empirical study are discussed and the gap between the most applied information security theories and real-life complexity is attempted to fulfil. The results are addressed through the theoretical framework.

This chapter aims to give an answer to the research questions for this study: and *"How employees experience the ISO 27001 standard's implementation in a software development environment?, "What kind of conflicts might appear between ISO / IEC 27001 standard requirements and day-to-day work?"* and *"How the target unit resolves the conflicts between ISO/IEC 27001 standard requirements and day-to-day work?"*. In subchapter 6.1. the findings of the study are discussed. In subchapter 6.2. the limitations of this study are discussed and in subchapter 6.3. the suggestions for further studies are presented.

6.1 Discussing the findings

In this subchapter the research findings are further discussed. The themes in this subchapter are organized in a same order as in the results chapter. Firstly, the contextual changes between the two interview rounds are discussed. Secondly, the employees' experiences of ISO 27001 standard's suitability to their software development environment are discussed. Thirdly, the emerged conflicts and their resolutions are discussed. Aspects related to improvements in information security are reviewed and compared to the previous literature. The weakness of the previous literature was that none of the previous theories could address the standard process in its complex nature. Therefore, a longitudinal case study was needed to follow the conflict resolutions and information security culture changes in a software development company.

6.1.1 Contextual changes between interview rounds

Soliman and Rinta-Kahnila (2020) described a context as the organizational environment and the background story in which the changes are happening. They described it as a debatable concept that can refer to various things, including geographical context, temporal context, or cultural context. It was noted that a context can give the change process frames that help in understanding the situation and phenomenon more deeply. Therefore, the organizational environment and the background story of the target organization were investigated through the interviews. In each interview rounds the same background questions were asked to clarify the context for the changes that are happening in. The changes in the employees' answers also show changes that have happened in the background during ISO 27001 implementation process.

The target organization Securitym was in a unique setting before the ISO 27001 standard implementation: a bigger ICT-organization had acquired the software development company and merged it to their own software development unit. Still, the Securitym and target unit felt as the target unit was working as their own unit. In addition, Securitym had the ISO 27001 certification already, but the target unit had never been ISO 27001 audited before.

Throughout the interview rounds, there were major changes noticeable related to the themes that were discussed. ISO 27001 standard implementation seemed to affect the target unit's information security culture, employees' information security policy familiarity, employees' perception of information security's presence in daily work and employees' attitudes towards ISO 27001 necessity to their organization.

One of the themes related to the organizational environment and background story were the organization's information security culture. During the ISO 27001 implementation the interviewees noticed that their information security culture has grown stronger. The narration related to security culture changed to more serious and collective. For example, one of the interviewees described how they do not have an information security architect since everyone is accountable for information security. This shows a major solidarity increase in addition to the overall change in information security culture's seriousness. ISO 27001 forces the organization to consider their own information security processes and find a way to document them in a mutual understanding. In the literature review, it was noticed that positive information security culture can affect the employees' information security compliance. As the culture changed in the organization, the ISO 27001 standard's effect can be perceived as positive.

The second theme that was discussed related to the context was the employees' familiarity with the information security policies. In the first interview round, seven of the employees thought they are familiar with the current information security policy. After the ISO 27001 implementation and auditing this number increased to nine. On the other hand, many interviewees mentioned how the information security policy is present in the beginning of their employment but then it gets forgotten. To avoid this, it would be important that the organization would regularly remind the employees of the information security policy or have regular training sessions related to the security policies. The challenge in getting the employees to update their knowledge of the security policies might be related to the organization's structure. Couple of interviewees mentioned how they have organizational level information security policies and then their own secure software development policies. The multiple policies should at least be kept short and comprehensible, so that it is possible for employees to update their policy knowledge.

The third theme that was discussed during the interviews was employees' perception of information security in their daily work. During the first interview round, eight of the interviewees felt that information security is present in their daily work. In the second interview round, all the interviewees felt that information security is present in their daily work. Many employees described how information security is linked to everything they do, and it is always tied to the processes. As the ISO 27001 standard forces the organization to observe and evaluate their information security processes, they might become more visible to employees. It can be speculated that when the employees have to document the information security measures they use, they recognize them more easily and are more aware of them daily. ISO 27001 might be a trigger to an organization to actively consider information security.

The fourth theme that was brought up in the interviews was a main motivator for employees' information security compliance. In the literature review, multiple theories of information security policy compliance were identified. To understand the employees' behaviour and organization's culture better, the interviewees were asked to explain what motivates them to comply with their organization's information security policies. In the first interview round, motivators like sense of duty, fear of risks, fear of dishonour, organization's reputation's importance, respect towards rules in general and conscientiousness were identified. In the second interview round the answers remained around sense of duty and fear of risks or dishonour. In addition to these, organizational culture and trust were added by two interviewees. Morale which was included into the theoretical review was present in the interviewees' answers but not clearly distinctive.

Many of the interviewee's descriptions can be generalized to sense of obligation towards the employer. According to Leach (2003) the employees who are happy with their employer's treatment usually feel more obligation towards their employer and therefore feel more pressured to behave in a desired way. Furthermore, the positive information security culture that was mentioned during the interviews is linked to the Theory of Planned Behaviour which underlined the information security culture's importance in employee's compliant behaviour.

Fear was identified in many answers and this links to two theories found in literature review: Rational Choice Theory and Protection Motivation theory. Both these theories underline the possible consequences of not behaving safely. Fear of the consequences can have a major impact on the compliance. In this research, the feared consequences were focused on risks and dishonour. It could be beneficial for an organization to present the possible consequences of information security breach to increase the employees' ISP compliance. On the other hand, fear can also be paralyzing and lead to a situation where employees are too scared to act. There were also factors which were not identified in the literature review. For example, conscientiousness and trust were not presented in the literature review but were still relevant motivators to two of the interviewees after the ISO 27001 implementation. Conscientiousness can be classified as a personal trait which might appear in many fields of employees' life. Trust is a more complex motivator which could be useful to study more in the future.

The fifth theme of the background questions was about employees' perception of ISO 27001 standard necessity. The interviewees were asked to evaluate what ISO 27001 standard might bring to the target unit and how it could affect the employees' daily work. The employees' perception of the ISO 27001 standard changed positively distinctly throughout the interviews. After the ISO 27001 implementation nine of the ten interviewees perceived ISO 27001 as necessary to their organization. The main themes that interviewees brought up related to the standard's necessity were clearly documented processes, more specifically identified and increased information security, and marketing advantage. Some of the interviewees were worried about the bureaucracy that the standard might bring with it and if the information security measures would fade into the background again. Rational choice theory argued that people aim to maximize their personal benefits while minimizing their costs. Thus, if the processes become more stiffer, the new practices might fade into the background again. After the implementation, the assessment was more positive, and the employees did not feel too overwhelmed with the new practices. It should be noted that between the interviews were only three months, hence it is impossible to evaluate if the changes are going to stay in the long term.

6.1.2 Experiences of ISO 27001 standard's implementation in software development environment

First research question in this study was: "How employees experience the ISO 27001 standard's implementation in a software development environment?". The interviewees brought up themes related to ISO 27001's suitability to software development environment, management's support during the implementation process and differences between experienced level of communication between managers and employees. Employees described the implementation process as challenging and even exhausting but they found strength from their good team spirit and everyone's investment.

Based on the employees' experiences, even ISO 27001 standard claims to be designed in a way where it is flexible enough to be used by every type of an organization, it does not seem to fit software development environment straightforwardly since it is not written from a software development's perspective. Nonetheless, many software development companies might need the ISO 27001 certificate to take part to competitive tendering. Like discussed during the interviews, some organizations require the certification before a software company can even participate to the competitive tendering. Particularly ISO 27001's deficiency comes notable when an organization does software development for individual customers. The ISO 27001's requirements are challenging to meet during an individual project. For example, if the customer is not willing to pay for security testing, the development team must skip that process. This might reduce the software's information security and then the software company does not follow the ISO 27001 guidelines. Hence, the organization is in a situation where it cannot meet customer's or standard's requirements at the same time. To ease organizations' information security documentation, ISO 27001 standard should be refined to more adjustable format to fit variety of organization working around different projects in different organizational cultures.

Other experiences related to ISO 27001 standard that the interviewees brought up was management's support in the implementation process. ISO/IEC 27001 (2017) emphasizes management's commitment to information security, so the management system has an actual opportunity to influence and act in the organization. The standard advises to use resources to run security awareness training which is designed to raise awareness and motivation about the organization's security policies and practices among employees and critical stakeholders. (ISO/IEC 27000, 2018.) Top management's support is emphasized in many studies but still in practice, its success hard to observe. In this study, the employees felt like the top management's support could have been improved. They especially hoped for management's guidance and resources to hire a consultant to make the standard implementation easier. In addition, there was no training related to ISO 27001 standard unless an employee was a part of the auditing. Furthermore, some employees felt that the communication related to the implementation process was lacking and they were not familiar with the process' progression. On the contrary, team leaders felt like the communication with employees was sufficient and successful. A similar finding was made in Hsu's (2009) study where employees' and managers' experiences of the information security management standard implementation's communication were totally different. This phenomenon could be avoided if managers informed the employees about the progress and stages and asked regularly if the employees needed more information. On the other hand, in Hsu's study the employees felt like they are not involved with information security at all. In this study, employees felt responsible for information security in their unit.

Team leaders were also praised. According to interviewees, team leaders were able to justify the standard implementation to employees and keep them motivated. It is important that standards and policies are justified to the employees to make them involved. Even if the top management's support was not optimal, employees in the implementation team got highly involved with the standard implementation process since that way they could affect how the new processes and practices affecting their daily work are constructed. Both team leaders and employees reported how their team spirit got them through the process even it was described as burdensome.

Overall, it seems that good project management practices can also make the ISO 27001 implementation less challenging. Top management's support, good communication between top management and employees, employees' involvement and sufficient training could make the implementation process more likely succeed. It may be difficult to fit ISO 27001 standard to software development environment, but an involved implementation team and a defined scope seem to improve the process. In addition, a consultant who is familiar with ISO 27001 implementation can offer a huge assistance to employees working around the standard. Although the standard certification might take a lot of resources and make the employees drained, it can offer a great opportunity to evaluate the organization's information security practices. ISO 27001 standard makes the organization allocate resources to improve and document the best information security practices which otherwise might be overlooked.

6.1.3 Conflicts and resolutions

Second and third research questions handled the conflicts that might appear between ISO 27001 standard requirements and daily work and how the conflicts were resolved. This subchapter discusses the two research questions: "What kind of conflicts might appear between ISO / IEC 27001 standard requirements and day-to-day work?" and "How the target unit resolves the conflicts between ISO / IEC 27001 standard requirements and day-to-day work?". These two questions formed the process part of the research's theoretical framework. Process in a contextual sense means a sequence of actions and events which is being used to explain the origins and outcome of the phenomena.

In this study, the conflict origin was identified in the code reviewing process. Securitym's software development unit is expected to practice code reviewing but since it was too burdensome to follow, the process was slowly forgotten. Employees working with software development hoped for a better code reviewing process and targeted their hopes to ISO 27001 standard: employees hoped the standard would make the unit consider their code reviewing processes meticulously. The conflict arose when the ISO 27001 standard's code reviewing requirements were hard to interpret. Interviewees criticized how the standard could be translated in many ways and how the standard does not state how to improve their processes. Pair programming, code reviews and testing can be part of secure development but the issue that arise in the target unit was that ISO 27001 did not define how secure development can be defined as secure. ISO 27001 mentions how code reviewing can rely on known mechanism and this is how the target unit resolved the conflict: they developed their code reviewing processes around vulnerability lists like OWASP Top 10 and SANS. These lists can be helpful, but ISO 27001 should clarify for example which known mechanism are acceptable to reduce confusion.

Another identified conflict was related to disciplinary measures. ISO 27001 standard requires disciplinary measures and processes to be documented and clearly communicated to employees. Disciplinary measures can be perceived as justifiable since General Deterrence Theory is widely used in information security research and its developer Gibbs (1975) argues that the stronger the severity and certainty of sanctions are for unwanted behaviour, the more individuals are deterred by it. According to D'Arcy and Herath (2011) the higher the risks, e.g. for punishments, are the more likely the person does not commit the crime. In this research, any kind of punishments caused a lot of disagreement among the employees. ISO 27001 demands that an organization must have an organization culture-based and systematic approach and framework for security design, implementation, monitoring and development. Employees felt like the disciplinary measures do not fit to Finnish organization culture or their own organizational culture at all, since in their culture leadership is more appreciated than management.

Disciplinary processes could be more relevant in other cultures and work environments but in the studied organization employing specialists, it can be highly unmotivating and cause backslash. During this study, it was clarified that the target unit did not handle the disciplinary process documentation, but the organization's management had dealt with it. However, interviewees recalled that there has been no clear communication of the disciplinary measures. It seems that the organization had to answer to the unsuitable standard requirements but after the auditing the disciplinary measures got relegated to the background. This is an understandable compromise from an organization which must balance between the standard requirements and motivational organization culture.

Through these two most visible conflicts, ISO 27001's duality was identified. Duality, an instance of opposition between two concepts of something, can be hard to resolve when the aim is to answer all requirements and get the certification. Unfortunately, ISO 27001 standard did not guide employees on how to make their information security processes better. Employees had to figure the best code reviewing processes out themselves and the standard had to be interpreted to the best of employees' ability. On the other hand, ISO 27001 standard has requirements that do not fit into every organization and culture. The disciplinary actions had to be documented, but employees felt like disciplinary measures would be highly unmotivating and some even told they would consider resignation if disciplinary measures would get more attention in the organization.

These conflicts identified bring up the feature that Siponen (2006) criticized about standards: standards focus on the existence of the process but not its actual content. Standards discuss what should be done, but not how these requirements should be executed. When a different business environment is added to it, interpretation becomes very difficult. While standards do not claim to be anything more, they could be more useful and usable if processes' contents would be communicated more unambiguously. ISO 27001 standard might be easier to implement when a consultant is hired but it should be made possible for every organization to implement the standard without a consultant or a massive amount of speculation. In addition, it seems that ISO 27001 does not take different kinds of organizational cultures into consideration and it tries to fit into every organization model which seems to be impossible.

After a long implementation process, the target unit was able to create their own processes that met the standard requirements since the auditing was successful and they got ISO 27001 certified. The changes were successful as the interviewees evaluated that their information security had increased, and employees paid more attention to information security policies and secure software development practices. The main lesson that the target unit seemed to learn during the ISO 27001 implementation was that there are many paths to the same end result, since the standard's requirements can be interpreted and every organization does not have to execute the processes in a similar way. It would be even better for organizations working in different business environments, that a more variable requirement list could be conducted, so the organizations could decide which requirements are possible to execute in their organizational culture and environment.

6.2 Limitations

In this subchapter this study's limitations are discussed. Like in every research, this study had its limitations which may influence the study's generalizability and reliability. The limitations that were identified were related to single case approach, sampling size, scope and changes due to the Covid-19 pandemic.

The first limitation is related to the single case study in one organization. When researching only one organization, the results could be more comprehensive. As only one part of the organization was researched, the comparison could not be conducted which leads to unilateral results. As the organizational setting was particularly unique hence the corporate acquisition and only the target unit's employees were interviewed, the culture might differ from organizations that are built differently. On that account, the results of this study might not be as generalizable.

The second limitation is the size of the sampling. Number of the employees interviewed was narrow due to resource limitations of this study. On the other hand, the target unit did not have a huge amount of employees so the sampling size could be evaluated as fitting compared to that. As mentioned in the research method chapter, there is no predetermined sample size in qualitative research. Nonetheless, for the purpose of this study and its contextual nature, the sample size served is adequate.

The third limitation is related to the scope of this study. Throughout literature review and two interview rounds with 10 interviewees, there was a massive amount of research material gathered in form of research articles, organization's web pages, interview records and spelled interview records. Due to the nature of master's thesis, the scope needed to be narrowed down to the themes that were discussed in this study.

The last limitation that was identified is related to Covid-19 pandemic which was prevailing during 2020. Covid-19 might have affected the standard implementation process since almost all the interviewees were working remotely from home. A lot of silent knowledge and opinions might have been not shared. On the other hand, this could make the interviewees' answers more reliable since corridor discussions might have affected their opinions and attitudes related to ISO 27001 implementation. In addition, Covid-19 pandemic changed the interview settings. The interviews were meant to be conducted in person, but remote interviews were held to avoid the spread of the virus. This could affect the interview results since the interview topics were sensitive in nature and some employees might not be as comfortable sharing sensitive information and opinions through communication applications to a person who they have never met in person.

6.3 Suggestions for further study

In this study, an organization had acquired a software development company and tried to get them ISO 27001 audited as well. During the ISO 27001 standard implementation two interview rounds were conducted. It would have been interesting to continue the longitudinal study to observe if the new processes and practices would stick to the target unit's daily practices. In the target unit's past, new policies had been soon forgotten and were no longer used. It would be important to examine how permanent the changes made due to the implementation of ISO 27001 are.

In addition, it would be beneficial to see if the information security management standard improves employees' compliance in practice since employees' own perception might differ from reality. This could provide a new perspective for evaluating information security management standards in practice.

Another suggestion for further study is to conduct a similar study with a bigger sampling. This study's sampling was rather small, and with a bigger sampling size it could be generalized into another software development companies that are aiming to get ISO 27001 certification. Studying different organizations in different industries could create more generalizable results.

Case studies about information security management standard implementation should be further developed. This study worked as an example in observing the duality between information security management standard requirements and practical demands. Since information security standards focus on the required processes’ existence and not their content, research that would illuminate different resolutions to meet the standard requirements would help organizations applying the certification. In addition, it would also enrich research in this field and possibly even help in classification of conflict resolutions.

7 CONCLUSIONS

The aim for this master's thesis was to demonstrate how complicated an ISO 27001 standard implementation can be in an organization which's industry does not match with the standard requirements' context straightforwardly. The research questions for this study were "How employees experience the ISO 27001 standard's implementation in a software development environment?", "What kind of conflicts might appear between ISO / IEC 27001 standard requirements and day-to-day work?" and "How the target unit resolves the conflicts between ISO / IEC 27001 standard requirements and day-to-day work?". These themes were studied through a literature review and an empirical study. The empirical study was conducted as a qualitative longitudinal case study which's target was Finnish ICT-organization's software development unit. The data was gathered through semi-structured interviews through two different interview rounds with timespan of three months. The interviews were constructed based on deficiency in the current IS literature.

As organizations are becoming more dependent on information systems, the importance of protecting information's availability, confidentiality, and integrity increases. One of the biggest information security management tools are information security management standards. Like other information security management standards, ISO 27001 focuses on the existence of the processes and not their content and quality. This study and its results are important for organizations implementing ISO 27001 standard in software development environment and the results can offer support to implementation team before and during the implementation process.

The study's structure was arranged from theory to empirical research. In the second chapter of this study, the main concepts including information security, security threats, insider threats and information security management standards were identified to define the terms and concepts discussed in this study. In the third chapter, the core research themes were identified, and the most applied information security compliance theories were presented. The fourth chapter handles the empirical research and its methods, subject and analysis. In the fifth chapter, the results of the empirical study are discussed. The seventh chapter discusses and analyses the results. The final chapter concludes the study.

This study aimed to find answers for the research questions and fill in the practical experiences of information security management standards missing from IS research by conducting an empirical study. The empirical study was based on the theoretical framework and gaps between the literature and practical experiences. Since the most applied theories were not sufficient to handle ISO 27001 standard implementation's impact on employees' experiences and practices, the empirical research tried to form a profound portrayal of the implementation process. The themes shifted between the two interview rounds since the first interview round's results affected the themes that were discussed in the second interview round. Even that qualitative case studies are not always generalizable or universal, the findings of this study can aid other software development units or companies that pursue ISO 27001 certification.

For the empirical research, ten employees of the Finnish ICT-organization's software development unit were interviewed in two interview rounds. As the sampling of this research was quite small, the findings of the study may not be as generalizable. However, the findings address the problematic nature of information security management standards and bring the employee aspect to the research. The findings could be more universal if more organizations could have been interviewed to get a more diverse viewpoint to the topic.

The three research questions were answered by observing different themes related to employees' experiences of the implementation process and changes in the security environment, conflicts between ISO 27001 standard's requirements and practical work's requirements and the resolutions to the emerged conflicts. One of the main findings was that ISO 27001 does not translate to software development environment straightforwardly. For example, there were difficulties related to customer projects in which customer decides if for example security testing is executed to the developed software.

One of the main issues was also related to the duality in ISO 27001 standard. It required disciplinary measures to be documented and communicated but the interviewees found disciplinary measures to be unmotivating and even repulsive. The target unit's daily work and culture did not meet with the standard's requirements. The resolution was to leave the sanctions uncommunicated. On the other hand, employees hoped that ISO 27001 would guide how code reviewing practices should be conducted, but it failed to do so. Hence, the standard did not answer to the practical demands. In organizational level, some of the interviewees hoped for better communication and guidance from the management. Especially a need for a consultant was brought up. Employees working with the standard implementation had to do a lot of interpretation and work as a team to clarify the context and scope of the standard.

Fortunately, the implementation team succeeded, and the standard auditing passed. The interviewees had positive experiences of the ISO 27001 standard even various conflicts arose. It was described how ISO 27001 auditing makes the organization allocate resources to evaluate and improve information security processes. The implementation team was conducted from employees working with software development so they could affect the processes that are going to impact their daily work. This way the employees were involved and motivated to make the information security processes suitable for their work. In addition, ISO 27001 seemed to positively affect the organization's security culture and employees' information security policy knowledge. ISO 27001 implementation process made the employees more conscious about information security and it changed few employees' main motivators for information security policy compliance.

Overall, ISO 27001 standard can be a good guideline for an organization to evaluate their information security processes. The results propose that ISO 27001 can improve information security awareness among employees and make them more familiar with the information security policies. ISO 27001 standard still carries the same demerit as other information security management standards: it focuses on the existence of process and not its contents. In practice, it could be more important to focus on improving information security and make the processes beneficial as possible instead of only listing the processes. Standards' nature is to answer the question "What?" and not "How?" but more practical requirement documentation could be a relief to certain organizations.

This research was conducted as a longitudinal research in three-month span. It would be interesting to observe an organization for a longer period to identify if the processes and practices developed for ISO 27001 auditing would remain in daily work. This could provide an interesting perspective for evaluating information security management standards in practice. In addition, since the sampling for this study was quite small, a similar study among multiple organizations should be conducted to make the results more generalizable. In-depth experiences can help other organizations and practitioners before and during the implementation process. More experienced researcher could even guide the organizations applying information security management standards.

REFERENCES

Al-Ghaith, W. (2016). Extending protection motivation theory to understand security determinants of anti-virus software usage on mobile devices. *International Journal of Computers, 10*, 125-138.

Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice.* Second Edition. Syngress: Elsevier, Inc.

Aytes, K. & Connolly, T. (2004). Computer Security and Risky Computing Practices: A Rational Choice Perspective. *Journal of Organizational and End User Computing, 16(3),* 22-40.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50(2)*, 179-211.

Baum, T., Liskin, O., Niklas, K. & Schneider, K. (2016), A Faceted Classification Scheme for Change-Based Industrial Code Review Processes. *IEEE International Conference on Software Quality, Reliability and Security (QRS)*, Vienna, 2016, 74-85.

Benbasat, I., Goldstein D. & Mead M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly, 11(3)*, 369-386.

Berner, A.S. (2011). Crossing the line: a survey on Finnish moral standards. Helsingin Sanomat, 5.11.2011. Retrieved 7.4.2020 from http://web.archive.org/web/20120610095324/http://www.hs.fi/english/article/Crossing+the+line+a+survey+on+Finnish+moral+standards/1135269828887.

Blume, L.E. & Easley, D. (2008). Rationality. The New Palgrave Dictionary of Economics , 2nd Edition.

Briney A. (2001). Information security industry survey. Information Security, October 2001.

Chan, M., Woon, I. & Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of information privacy and security, 1(3),* 18-41.

Chenoweth, T., Minch, R. & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. *Proceedings of the 42nd Hawaii International Conference on System Sciences.*

Darke, P., Shanks, G. & Broadbent, M. (1998) Successfully completing case study research: combining rigour, relevance and pragmatism. *Info Systems, 8,* 273-289.

D'Arcy, J. & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems, 20*, 643–658.

D'Arcy, J., Hovav, A. & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research, 17(1)*, 79–98.

Eisenhardt, K. (1989). Building Theories from Case Study Research. *The Academy of Management Review, 14(4),* 532-550.

Eisenhardt, K. & Graebner, M. (2007). Theory Building from Cases: Opportunities and Challenges. *Academy of Management Journal, 50(1)*, 25–32.

Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2005). A management perspective on risk of security threats to information systems. *Information Technology and Management, 6(2-3),* 203-225.

Gibbs, J.P. (1975). *Crime, punishment and deterrence*. Elsevier.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & security, 73*, 345–358 .

Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. (2008). Combating the insider cyber threat. *IEEE Security & Privacy, 6(1).*

Haidt, J. (2012) *The Righteous Mind: Why Good People Are Divided by Politics and Religion.* New York: Pantheon Books.

Herath, T. & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47(2),* 154-165.

Hirsjärvi, S. & Hurme, H. (2001). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö*. Helsinki: Yliopistopaino.

Hsu, C. (2009). Frame misalignment: interpreting the implementation of information systems security certification in an organization. *European Journal of Information Systems, 18,* 140-150.

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees?. *Communications of the ACM, 54(6),* 54-60.

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical report, 13,* 247–255.

Humphreys, E. (2011). Information security management system standards. *Datenschutz und Datensicherheit-DuD, 35(1),* 7-11.

International Organization for Standardization - ISO. (2017). *Information technology -- Security techniques -- Information security management systems -- Requirements* (ISO/IEC Standard No. 27001). Retrivied on 25.3.2020 from https://www.iso.org/standard/54534.html

International Organization for Standardization - ISO. (2018). *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary* (ISO/IEC Standard No. 27000). Retrieved on 25.3.2020 from https://www.iso.org/standard/73906.html

Jai-Yeol, S. (2011). Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to Follow IS Security Policies. *Information &. Management, 48(7),* 296–302.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science, 32*, 489-496.

Kankanhalli, A., Teo, T., Tan, B.C.Y. & Wei, K.W. (2003) An integrative study of information systems security effectiveness. *International Journal of Information Management, 23,* 139-154.

Khan, S., Long, C. & Iqbal, S. (2014). Top Management Support, a Potential Moderator between Project Leadership and Project Success: A Theoretical Framework. *Research Journal of Applied Sciences, Engineering and Technology. 8,* 1373-1376.

Kirlappos, I., Beautement, A., & Sasse, A. M. (2013). 'Comply or Die' Is Dead: Long Live Security-Aware Principal Agents. *Financial Cryptography and Data Security,* Springer, 70–82.

Lambo, T. (2006) ISO/IEC 27001: The future of infosec certification. *The ISSA Journal, 4(11),* 44-45.

Leach, J. (2003). Improving user security behaviour. *Computers & Security, 22(8),* 685-692.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *Mis Quarterly,* 173-186.

Moody, G. D., Siponen, M. & Pahnila, S. (2018). Toward A Unified Model of Information Security Policy Compliance. *MIS Quarterly, 42.*

Oladimeji, E.A., Supakkul, S., & Chung, L. (2006). Security threat modelling and analysis: A goal-oriented approach. ICSE 2006.

Pahnila, S., Siponen, M. & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *System sciences, HICSS 2007*, 156b-156b, IEEE.

Pettigrew, A. (1985). Contextualist research and the study of organizational change processes, *Res. Methods Inf. Syst.*, pp. 53-78

Pfleeger, S.L., Sasse, M.A. & Furnham, A. (2014). From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Homeland Security & Emergency Management, 11(4)*, 489–510.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & security, 23(8),* 638-646.

Puhakainen, P. & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly, 757-778.*

Raggad, B. (2010). *Information Security Management: Concepts and Practice.* CRC Press: Taylor & Francis Group, LLC.

Ramamurthy, Y. & Wen, K. (2012) Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems, 29(3)*, 157-188.

Saaranen-Kauppinen, A. & Puusniekka, A. (2006). KvaliMOTV - Menetelmäopetuksen tietovaranto [online publication]. Tampere: Yhteiskuntatieteellinen tietoarkisto.

Sarajärvi, A., & Tuomi, J. (2017). *Laadullinen tutkimus ja sisällönanalyysi: Uudistettu laitos.* Tammi.

Siponen, M. (2000). A Conceptual Foundation for Organizational IS Security Awareness. *Information Management and Computer Security, 8(1)*, 31–41

Siponen, M. (2006). Information security management standards focus on the existence of process, not its content. *Communications of the ACM, 49*, 97-100.

Siponen, M. & Vance, A. (2012). IS Security Policy Violations: A Rational Choice Perspective. *Journal of Organizational and End User Computing, 24(1).*

Soliman, W. & Rinta-Kahila, T. (2020). Toward a refined conceptualization of IS discontinuance: Reflection on the past and a way forward. *Information & Management, 57(2).*

Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security, 7(1),* 50-57.

Solms, S.H. & Solms, R. (2009). Information Security Governance. 10.1007/978-0-387-79984-1.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & security, 24(2),* 124-133.

Stevens, B. & Brownell, J. (2000). Ethics: Communicating standards and influencing behavior. *Cornell Administration Quarterly, 41(2),* 39-43.

Theoharidou, M., Kokolakis, S., Karyda, M. & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security, 24(6)*, 472-484.

Tittle, C. R. (1995). *Control balance: Toward a general theory of deviance.* USA: Westview Press.

Van Bruggen, D., Liu, S., Kajzer, M., Striegel, A., Crowell, C. & D'Arcy, J. (2013). Modifying smartphone user locking behavior. *Symposium on Usable Privacy and Security, 10*, 1–14.

Vroom, C. & Solms, R. (2004). Towards information security behavioural compliance. Computers & Security, 23, 191-198.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18(2),* 101-105

Williams, E. J. , Noyes, J., & Warinschi, B. (2018). How Do We Ensure Users Engage In Secure Online Behavior? A Psychological Perspective. Conference on Cognitive and Behavioral Psychology 2018.

Whitma, E. (2003). Enemy at the gate: Threaths to information security. *Communications of the ACM, 46(8),* 91-95.

Woon, I., Tan, G.W. and Low, R.T. (2005). A protection motivation theory approach to home wireless security. *Proceedings of 26 th International Conference on Information Systems,* 31.

Zinatullin, L. (2016). *The Psychology of Information Security : Resolving Conflicts Between Security Compliance and Human Behaviour.* IT Governance Publishing.