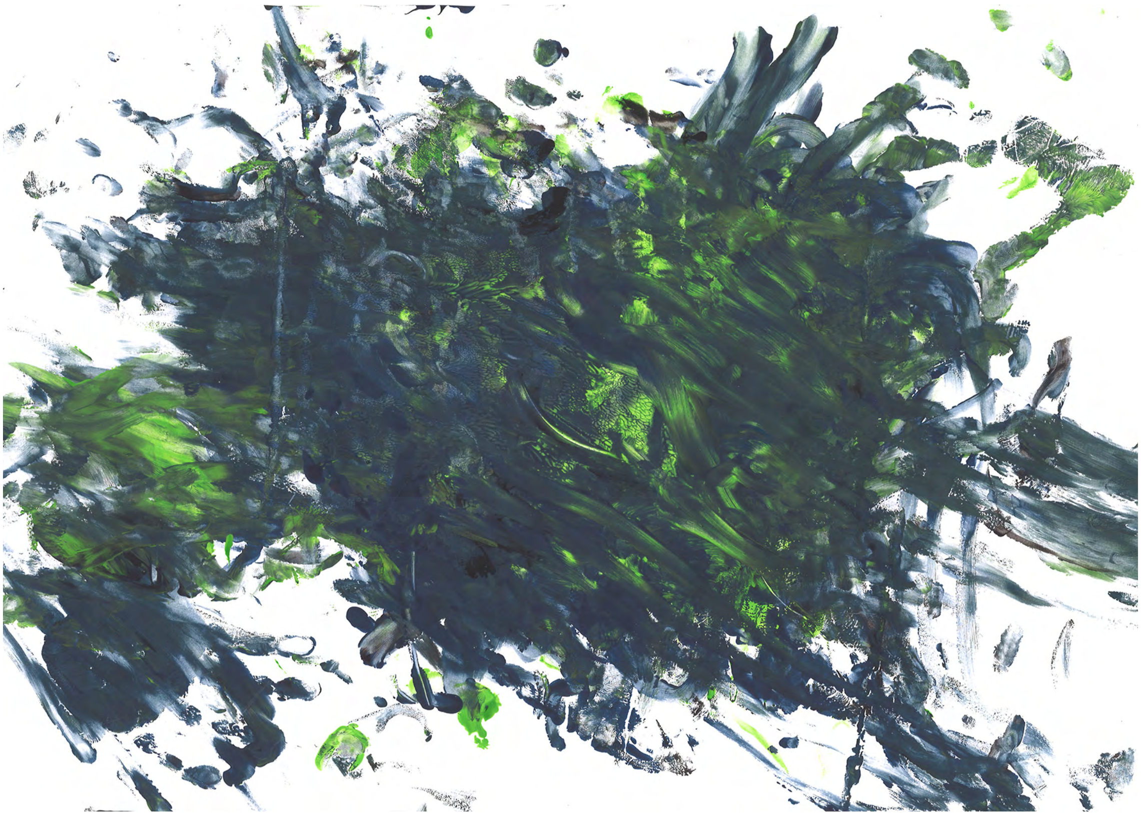
JYU DISSERTATIONS 607

Hanna Paananen

Information Security Policy Development

Considering the Practices of Making Rules



UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION
TECHNOLOGY

JYU DISSERTATIONS 607

Hanna Paananen

Information Security Policy Development

Considering the Practices of Making Rules

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi Agoran auditoriossa 2
helmikuun 17. päivänä 2023 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, auditorium 2, on February 17, 2023, at 12 o'clock.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2023

Editors
Marja-Leena Rantalainen
Faculty of Information Technology, University of Jyväskylä
Päivi Vuorio
Open Science Centre, University of Jyväskylä

Cover picture by Pekka Paananen.

ISBN 978-951-39-9297-2 (PDF)
URN:ISBN:978-951-39-9297-2
ISSN 2489-9003

Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-9297-2

ABSTRACT

Paananen, Hanna
Information security policy development – Considering the practices of making rules
Jyväskylä: University of Jyväskylä, 2023, 100 p.
(JYU Dissertations
ISSN 2489-9003; 607)
ISBN 978-951-39-9297-2 (PDF)
Diss.

Information security policies (ISPs) are at the core of organizations' information security efforts. They set objectives for protecting information assets and direct employees to achieve these goals. Advice for ISP development is available both in research and best practice literature. A common approach to describing ISP development is a lifecycle model that depicts inputs such as assessments, the ISP creation, and outputs that are implemented and maintained until the cycle starts again. However, ISP development needs to be planned to support the business requirements by adapting the method and the resulting policy to fit the context. The rules that are created in this process must be well considered so that employees are able to follow them in their daily work without conflicts with their other duties.

This dissertation presents an action research study on ISP development. Its theoretical base is constructed around the idea that the ISP subject is a moral thinker who will make decisions about complying with rules by weighing options to reach the best possible results. This has implications for the ISP development process. The policy developers must be able to critically assess the alternatives for new rules based on their knowledge of the operations of the organization. In the study, the researcher helped a consultant firm to reconfigure their ISP development service to one that serves the client organization's information security needs better. A set of 11 critical considerations were introduced to support critical thinking during the development process. They were based on previous research and needs expressed by companies. The critical considerations were used to highlight issues in the ISP development that needed new practices to foster critical thinking. During four cycles of action research, new practices were formed in the ISP development process to improve the gathering of facts and employee opinions in the client organization.

This dissertation contributes to the current research on ISP development by presenting a way to convert general guidelines to local practices. The critical considerations can be used to further study the success of ISP development, and they can be easily implemented by practitioners in new contexts.

Keywords: information security, action research, moral thinking

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Paananen, Hanna
Tietoturvapolitiikkojen kehittäminen – Sääntöjen luomisen käytännön näkökohdat
Jyväskylä: Jyväskylän yliopisto, 2023, 100 s.
(JYU Dissertations
ISSN 2489-9003; 607)
ISBN 978-951-39-9297-2 (PDF)
Diss.

Tietoturvapolitiikat (TTP:t) ovat keskeinen osa organisaatioiden tietoturvatoimintaa. Ne asettavat tavoitteita tiedon turvaamiselle ja ohjaavat työntekijöitä saavuttamaan nämä päämäärät. TTP:n kehitykselle on tarjottu ohjeita niin tutkimuskirjallisuudessa kuin käytännön oppaissakin. Yleinen lähestymistapa TTP:n kehitykseen ovat elinkaarimallit, joissa kuvataan syötteitä, kuten arvioinnit, TTP:n luominen sekä tuotosten laittaminen käytäntöön ja ylläpitäminen kunnes sykli alkaa taas alusta. Jokaisella organisaatiolla on kuitenkin sille ominaiset liiketoimintavaatimukset, joiden vuoksi kehittäminen pitää suunnitella niin, että se tukee menetelmän ja syntyvän politiikan mukauttamisen kontekstiin. Tässä prosessissa luotujen sääntöjen tulee olla hyvin suunniteltuja, jotta työntekijöiden on mahdollista noudattaa niitä ilman, että ne ovat ristiriidassa heidän muiden velvollisuuksiensa kanssa.

Tässä väitöskirjassa esitellään TTP:n kehittämiseen liittyvä toimintatutkimus. Sen teoreettinen pohja rakentuu ajatukselle, että TTPn kohteena oleva henkilö käyttää moraalista ajattelua ja tekee päätöksiä sääntöjen noudattamisesta päästäkseen parhaaseen lopputulokseen. Tämä vaikuttaa myös TTP:n kehittämisprosessiin. Politiikan kehittäjien on voitava kriittisesti arvioida vaihtoehtoja uusille säännöille perustuen heidän tietämykseensä organisaation toiminnasta. Tutkimusprojektissa autettiin konsulttiyritystä rakentamaan uudelleen heidän TTP:n kehittämispalvelunsa sellaiseksi, joka vastaa paremmin asiakasorganisaation tietoturvatarpeita. Kriittisen ajattelun tukemiseksi kehitettiin 11 kriittistä näkökulmaa, jotka perustuivat aiemmalle tutkimukselle sekä yritysten esittämille tarpeille. Kriittisiksi näkökulmiksi valittiin sellaisia asioita TTP:n kehittämisessä, joihin tarvittiin uusia käytäntöjä tukemaan kriittistä ajattelua. Toimintatutkimuksen neljän syklin aikana TTP:n kehittämisprosessiin luotiin uusia käytäntöjä, jotta voitiin parantaa asiakasorganisaatiossa faktojen sekä työntekijöiden mielipiteiden kartoitusta.

Tämä väitöskirja edistää nykyistä TTP:n kehittämisen tutkimusta esittämällä tavan muuntaa yleisiä ohjeita paikallisiksi käytännöiksi. Kriittisiä näkökulmia voidaan käyttää TTP:n kehityksen onnistumisen jatkotutkimukseen ja ammattilaiset voivat ottaa ne käyttöön eri konteksteissa.

Asiasanat: tietoturva, toimintatutkimus, moraalinen ajattelu

Author

Hanna Paananen
Faculty of Information Technology
University of Jyväskylä
Finland
hanna.k.paananen@jyu.fi
ORCID 0000-0002-3005-4363

Supervisors

Mikko Siponen
Faculty of Information Technology
University of Jyväskylä
Finland

Marko Niemimaa
Department of Information Systems
University of Agder
Norway

Reviewers

Karin Hedström
School of Business
Örebro University
Sweden

Carol Hsu
The University of Sydney Business School
University of Sydney
Australia

Opponent

João Baptista
Management Science department
Lancaster University
United Kingdom

FOREWORD

This dissertation is an in-depth description of a research project in that I unexpectedly got involved in 2016. Eetu Luoma, my master's thesis supervisor, recommended me for a job on a project on information security – an unfamiliar research area for me at the time. I will always remember Eetu with gratitude for sparking my interest in research. From the beginning in those early days, this dissertation tells the story of how I formed my views on information security policies and their research and used what I had learned to make sense of what happened in practice.

I would like to thank my supervisors, Mikko Siponen and Marko Niemimaa, for their support and advice during this dissertation process. I am also grateful to Michael Lapke for his supervision in the first steps of this project. I would not have been able to come to terms with the theoretical aspects of this study without the discussions I had with my supervisors. My colleagues have also helped me, not alone, by being sounding boards to my ideas but also by sympathetically listening to my frustrations and telling me to keep going. Similarly, reviewers of my research papers have always given me invaluable advice that has helped me improve my work. Most importantly, I thank my external reviewers, Carol Hsu and Karin Hedström, and my opponent João Baptista for their helpful comments.

I am grateful for the project and grant funding I have received from the European regional development fund through Tekes (now Business Finland), the Finnish Cultural Fund (Central Finland fund), and the Faculty of Information Technology. Without their support, this research would not have been possible. Similarly, the contribution of the companies that participated in this project was not only vital for this study but will hopefully help the research field move forward in some way. I would particularly want to thank the two main informants at ISMcorp who patiently kept having conversations with me even when my questions were pointless.

I have not been able to do a single big (or even small) accomplishment in my life without the support of my family. My parents and sister have helped me with everything through this process, and a simple thank you doesn't seem enough. I met my husband just before I started the PhD program, and he too had to keep me going when all seemed lost. He has given me the strength to carry on and two beautiful children who have made this journey worthwhile. I dedicate this work to my sons, who were the reason why I pushed myself to write these last words in finally. I hope they will be proud of me someday.

The road to completing this dissertation has been long. It has been written in the courtyard of a hotel in Virginia, on a wildlife research station, at Swedish horse stables, and the newborn ICU. Needless to say, there have been ups and downs, but I never thought of quitting. Writing a dissertation is a learning process, and I took the time to learn.

Jyväskylä 26.12.2022
Hanna Paananen

Photo in series: "Pään sisältä syntyy teksti", Auli Dahlström

ACRONYMS

AR	Action research
CC	Critical consideration
CIA	Confidentiality, integrity, availability
IS	Information security
ISP	Information security policy
IT	Information technology

FIGURES

TABLES

CONTENTS

1 INTRODUCTION

The advancement of the information society has made information security (IS) important for both individuals and organizations. A dramatic shift toward an even more digitalized society was seen in 2020 when COVID-19-related lockdowns forced people toward remote work worldwide (Hantrais et al., 2020). At the same time, the number of cyber-attacks skyrocketed (Posey & Shoss, 2022), and, for example, in 2021, ransomware damages were estimated to cost 20 billion US dollars globally (Morgan, 2022). Thus, the increasing importance of information and diversifying ways of working create a need for organizations to have successful IS management to prevent losses and continue operations.

Organizations use IS policies (ISPs) to control the use of their information assets. An ISP is a statement of the goals for IS in an organization and the rules related to prevention, detection, and response to IS incidents (Baskerville & Siponen, 2002; Cram et al., 2017). On a higher strategic level, it is a statement from the organization's management on how the organization should operate relating to IS matters. On a lower operational level, the policy can state how work should be organized to achieve higher-level goals (Baskerville & Siponen, 2002).

In textbooks and research literature on IS, ISPs are described as the foundation of IS efforts of an organization and are thus basically mandatory (Goel & Chengalur-Smith, 2010; Raggard, 2010, p. 166; Straub, 1990). However, studies have found that many organizations manage to operate without one (Yildirim et al., 2011), or even more commonly, they have made a document called an ISP, but the statements on the policy do not translate into everyday compliance (Balozian & Leidner, 2017; Kolkowska et al., 2017; Posey & Shoss, 2022; Yildirim et al., 2011). This may be the case when ISP development has other objectives than IS, such as pleasing an external auditor (Siponen, 2006) or protection from legal consequences (Tuyikeze & Pottas, 2010).

It can be argued that the performance of the policy is already stipulated in its creation process. Among other things, comprehensiveness, fairness of the rules, easily readable documentation, applicability to the operations of the organization, and compliance with regulations are formed when the policy is created (Goel & Chengalur-Smith, 2010; Kolkowska et al., 2017). These factors affect how well ISPs are able to achieve IS goals (Cram et al., 2017). However, there is an abundance of literature on ISP compliance (Moody et al., 2018) and computer abuse (D'Arcy & Hovav, 2007; Straub, 1990), which focuses on understanding why people break IS rules. They mainly apply criminological and fear theories to improve employees' IS behavior (Haag et al., 2021; Siponen et al., 2022). These domains, as well as the literature on Internet-use policies (Li et al., 2014), often consider employees' noncompliance with ISP to be a user-related problem and not an issue stemming from the ISP itself (Bulgurcu et al., 2010; Jiang et al., 2021; Moody et al., 2018). That being said, some noncompliance issues can stem from the poor development of ISPs (Puhakainen & Siponen, 2010). Studying ISP development can also offer tools to improve ISPs, which in turn can help improve so-called employees' ISP compliance problems.

A number of general ISP development methods have been published in the research and best practice literature (for reviews see Cram et al., 2017; Klaic 2010; Paananen et al., 2020). There are some widely spread ideas of the matter, such as the cyclical development process (e.g. Flowerday & Tuyikeze, 2016; Knapp et al., 2009), which are based on practice or survey research. However, there have also been reports of a discrepancy between high-level policy development and its application in ground-level practical work (R. von Solms et al., 2011). This leads to situations where the organization has made an effort to develop an ISP, but it is difficult to implement as a part of everyday work due to disconnection to the context (Burgemeestre et al., 2013; Hedström et al., 2011; Karyda et al., 2005).

This dissertation focuses on the practical level of ISP development. As will be argued in the next section, the research approaches and processes at the higher methodological level of ISP creation have been well-established and are widely used by professionals. This study will focus on the practice-level execution of these methods and guidelines. There are still many unknown elements about the actual practices of the ISP development process, such as how to turn general process-level methods into work tasks, what role employee participation plays, and whether omitting or adding steps affects the result.

The focus of this study is to understand how general guidelines turn into real-world ISP development practices. This study aims to understand *what kind of support and advice previous research literature provides for ISP development*. Then, based on the answers to the previous question, we move on to find out *how we can improve the practices of organization-specific ISP development.*

Section 2 discusses the existing methods for ISP development and their underlying assumptions in the research literature. In section 3, previous research and the theory of making rules are used to provide a theoretical starting point for an action research (AR) study. In section 4, the research approach is introduced, and the results of the study are presented in section 6. Section 6 offers answers to the research questions and implications for research and practice.

2 ISP IN RESEARCH LITERATURE

ISPs have been widely discussed in both research and practitioner literature. This section will first introduce the complexity of the subject by studying the definitions given to the term ISP in the literature. Then, research on ISP development methods is presented. Lastly, we consider the ISP development process through the theory of making new rules. The following review of existing literature (pages 13-35) has partly been published in the article *State of the Art in Information Security Policy Development* (Paananen et al., 2020).

The literature for this review was searched following the guidelines provided by Levy and Ellis (2006). An initial search was conducted on Google Scholar using the search terms "information security policy" and "development" to find papers on ISPs and especially to find papers that would answer the research questions. Around 70 articles with promising topics were chosen, but upon closer inspection, most of the articles did not concern ISP development. After the Google Scholar searches, another search solely targeting academic literature was conducted using Elsevier's Scopus search engine (for search terms, see Appendix 1). This search included prominent journals in the fields of IS and information systems without limitations on the year of publication. The search yielded a list of 87 articles, which were then evaluated first by excluding clearly nonrelated papers by title and then by making a more detailed selection on the basis of the abstracts. The main reasons for exclusion were papers discussing ISPs but not their creation and purely technical approaches. However, some papers from the former group were included if they presented clear implications for ISP development. Then, a backward reference search was conducted on the sample articles using their reference lists to find promising topics. For the most promising articles, a forward-author search was also conducted to find recent papers written by those authors.

2.1 Defining the term “information security policy”

IS management has long been researched and developed in both industry and academia (Siponen & Baskerville, 2018). Instructions for ISP development have also been around for decades (Klaic, 2010; Olnes, 1994). The roots of some practices can be traced to protecting governmentally classified information in the 1960s and 1970s (Klaic, 2010). These days, IS has changed from being the interest of a small group of experts to something everyone must consider. The long history and increasing popularity of the topic have yielded a vast amount of research literature on the subject of IS and ISPs (Silic & Back, 2014).

Before we can study the ISP development process, we must first understand what is meant by the term ISP. In this section, we examine the definitions and functions of ISPs described in the literature. In many research articles, ISPs are not clearly defined, and a single definition has not become dominant. Existing studies have adopted different definitions of ISPs, and studying them can help us understand the different approaches that have been taken.

The term ISP has different meanings in computer science security and (management) information systems security(Siponen, 2005). Especially in computer science security literature, the term ISP may refer to a technical policy that can be implemented in an information system to control, for example, users’ access to information (Sandhu & Samarati, 1994). In addition to technical policies, the term “ISP” is also widely used in the IS management context (Baskerville & Siponen, 2002). Therein, an ISP refers to document(s) regulating human actions regarding IS or expressing the organization’s IS aims. This study focuses on this view of ISPs and excludes access control policies in database security. In addition, given the focus on organizational ISPs, governmental security policy development is outside the scope of this study.

In the ISP literature, the most-used terms are “security policy” and “information security policy.” Some authors use these interchangeably, while others stress the difference between them (Corpuz, 2011; Klaic & Hadjina, 2011). There are also different views on how IS–related directives should be connected to each other. Some authors recommend a policy architecture where policy documents from high strategic level to low-level operational policies are all linked together (Coles-Kemp, 2009; R. von Solms et al., 2011). Technical and managerial policies are often discussed separately but they are assumed to be interconnected (Baskerville & Siponen, 2002; Cram et al., 2017; Gritzalis, 1997). Some authors refer to ISPs only when talking about high-level policies; therefore, they exclude more specific guidelines or procedures because they are viewed as outside the scope of ISPs (Corpuz, 2011; Klaic, 2010; Rees et al., 2003).

2.1.1 Definitions and functions of ISPs

Because there is so much variation in the use of the term "ISP", it helps to gain an overall picture of the concept by examining the definitions and functions in detail. TABLE 1 summarizes the characteristics and functions of ISPs that were identified in the literature. The definitions and functions of ISPs are often not explicitly discussed in research articles. The reader is often expected to know what an ISP comprises of and what it is expected to do in an organization.

TABLE 1 ISP characteristics and functions

Theme	**ISP characteristics**	**ISP functions**
Steering the organization	Statement of security goals Guidance/instruction Statement of rules Communication tool	Supports business goals Control The basis for performance measurement Evidence of the IS program
The actor and the asset	Defines subjects Defines objects	State responsibilities and authority Provides an overview of information assets
Preparing for incidents	Comprehensive plan Addresses risks Recovery plan	The basis for security culture Prevents loss/misuse of information Ensures continuity

Steering the organization

An ISP can be a declaration of a desired state of security, and its contents have been described with words such as "security goals," "strategy," "objectives," "intentions," and "desirable achievements." Some definitions also mention policy as a reflection of values and beliefs (Hedström et al., 2011). Klaic (2010, p. 1204) describes this as follows: "The IS policy document in the narrow sense represents a statement or declaration of the most important management persons (CEO, Executive Board, Minister...), about beliefs, goals, and reasons, and also general ways to accomplish desirable achievements in the field of information security." Many authors also recommend that the ISP should maintain and complement the organization's overall business goals (Antón & Earp, 2001; Höne & Eloff, 2002). Saleh (2011) stated that the intention is not only to achieve security objectives (integrity, availability, and confidentiality, CIA) but also to ensure that the organization achieves its mission despite accidents and attacks. From a policy-architecture point of view, these goals are usually the purpose of higher-level documents (Baskerville & Siponen, 2002).

According to Corpuz (2011),an ISP offers a security direction for organizations to implement their IS management. An ISP can be viewed as a tool that management uses to communicate its vision and guide the rest of the organization (Sommestad et al., 2014). The instructions regarding actions (directions, guidance, procedures, instructions, and methods) are mentioned in many articles as part of the lower-level policies or guidelines (Cram et al., 2017; Karyda et al., 2005; Wood, 1995). For example, Cram et al. (2017, p. 607) described issue-specific policies as follows: "[they] include guidelines and procedures (i.e., acceptable use policies) that employees must adhere to in their daily interactions with information and technology resources.” von Solms et al. (2011) see ISPs as directives from executive management that are disseminated further into the organization via lower-level policies. The function of this policy architecture is to support comprehensive control over information use. An ISP can determine penalties and countermeasures if its terms are violated and can be seen as a precondition for implementing effective deterrents (Doherty & Fulford, 2005; Knapp et al., 2009; Rees et al., 2003). Another reason for having a documented policy is to protect the company in case there are legal disputes (Tuyikeze & Pottas, 2010). While deterrence by penalties is a popular topic in the compliance literature (Siponen et al., 2022), its counterpart, reward, is not as widely studied (Chen et al., 2012; Sommestad et al., 2014).

Describing acceptable behavior has also been mentioned in many articles, specifically the acceptable use of information technology (IT) (Galletta & Hufnagel, 1992; Sommestad et al., 2014). Many authors describe an ISP as a collection of rules (Yildirim et al., 2011) that explain in detail what to do (Burgemeestre et al., 2013). Instruction for an action may be considered the content of lower-level policies (Baskerville & Siponen, 2002).

An ISP is often considered to be the source of rules and protocols. Some think an ISP is a rulebook that needs to be followed by all who use the organization’s information (Yildirim et al., 2011). These rules may also be called procedures, and they may also be supplemented by guidelines on how they can be followed (Klaic, 2010). As the notion of power and agency of the policy subject differs between texts, so does the need for absolute rules versus tools for independent decision-making. Rule-based ISPs that demand precise compliance suit organizations that have stable environments and rule-oriented organizational cultures (Siponen & Iivari, 2006). It is suggested that organizations operating in unpredictable environments could adopt an ISP design for their organizations that allows for security-related decisions to be made while adapting to new situations (Siponen & Iivari, 2006).

Metrics can be formed to measure the stated procedures or tangible goals of a policy. von Solms et al. (2011, p. 3) explain measuring as a form of control: “Control is normally exercised by capturing data at the lowest levels of execution and control: measuring compliance against the Operational level policies. “Some have suggested general quantitative metrics that management can use to make IS decisions, such as the return on the security investment, fault tree analysis, and the certainty factor (Klaic, 2010).

ISP documentation works as a communication tool, not only for policy subjects but also for other stakeholders. An organization may develop an ISP to show evidence of its IS actions that comply with regulations and standards (Cram et al., 2017; Whitman, 2008). The evidence of being prepared for IS incidents may also be of interest to external stakeholders, such as customers and partners. An ISP is viewed as the foundation of the IS efforts in a company (Lopes & Sá-Soares, 2010), and a written policy can be accepted as proof that work has been done to improve IS. Evidence of an ISP may even be needed in a court of law if the company’s actions are challenged (Whitman, 2008).

Addressing the actor and the asset

Baskerville and Siponen (2002) use the terms "information security subjects" and "objects" to distinguish between the actors affected by the policy and the information assets being protected. The function of a policy can be to help all individuals affected by the policy (subjects) make decisions about their actions when handling information (objects).

The rights and responsibilities of the organization members are stated in the ISP to help them make future decisions when handling information (Baskerville & Siponen, 2002; Doherty et al., 2009; Siponen, 2005). It is important to remember that the policy is meant for the legitimate users of the information (Yildirim et al., 2011), which may also include users external to the organization. Some roles may also include the authority to make security decisions, approve other users' actions, and change the ISP (Goel & Chengalur-Smith, 2010; Ward & Smith, 2002; Wood, 1995). Some authors warn us about making overly simplistic assumptions about the authority of security decisions residing at the top tier of the organization and recommend an analysis of the actual power structure (Coles-Kemp, 2009; Lapke & Dhillon, 2008).

The objects of the policy are usually described as information assets, systems, and data. In their definition, Abrams and Bailey (1995, p. 128) focused on the object of the policy: "The policy should address the information assets of the organization, threats to those assets and the measures the management has decided are reasonable and proper to protect those assets." Some authors have also mentioned that the policy should not be technology-specific (Klaic, 2010; Rees et al., 2003). Listing the assets and their levels of protection can be useful to personnel enforcing ISPs (Lopes & Sá-Soares, 2010). Information is used by technology, stakeholders, and processes, which all affect the requirements for the protection of that information (Posthumus & von Solms, 2004).

Preparing and recovering from incidents

Creating an ISP is a way for the organization to plan ahead for the possibility that its information resources might encounter an attack or accident (Maynard et al., 2011). The ISP highlights executive management's commitment to security and envisages an "ideal" operational environment (Ward & Smith, 2002). The policy-planning process creates an understanding of the need for security and defines acceptable security levels to protect information (Klaic & Hadjina, 2011; Ward & Smith, 2002; Yildirim et al., 2011). ISPs may guide the IS culture and express the values of an organization (da Veiga & Eloff, 2010; Hedström et al., 2011). The ISP should create a secure environment where the privacy of its subjects and stakeholders is also considered (Talbot & Woodward, 2009).

The ISP can be derived from the strategic requirements for risk management (Corpuz, 2011), whereby the strategic-level decision-makers use the policy as a tool to reduce the risk to the company's information assets. ISP development methods are often described as starting from a risk analysis where the threats and vulnerabilities are determined to find the risks, and the policy is developed in order to stop these risks from being realized (Tuyikeze & Pottas, 2010). The most commonly used ways to describe risks to information are confidentiality, integrity, and availability (CIA) (Glasgow et al., 1992). Some authors add nonrepudiation to the list (Siponen & Oinas-Kukkonen, 2007) or substitute availability with assured service (Sterne, 1991) or identification and authorization (Trompeter & Eloff, 2001). Some authors, however, see this approach as being too IT-centered or vague (Dhillon & Torkzadeh, 2006; Doherty et al., 2009; Sterne, 1991). Many have adopted a broader view in which the planned protection and sharing of information is a vital part of creating business value (Ashenden, 2008).

In addition to preventing risks, ISPs may also serve as a plan to recover from materialized risks (Baskerville et al., 2014). It guides the investigation of security incidents and provides procedures, such as documenting the incident and containing it to limit further damage (Rees et al., 2003). A responsive way of dealing with risks is especially useful in organizations that operate in unpredictable markets (Baskerville et al., 2014). As information and IT provide companies with the means through which to operate and gain a competitive advantage, businesses must rely on their continuous availability, even when risks materialize. Company boards should be interested not just in good IT governance but also in IS to secure the continuation of business operations (Abu-Musa, 2010; McFadzean et al., 2007).

As companies' perceptions of risks, resources, and management styles differ, so do the different definitions and functions of ISPs. Due to these different views, the literature also provides multiple ways to develop an ISP that should fulfill expectations regarding its nature and use.

2.1.2 The definition used in this study

It is critical to have a mutual understanding of what an ISP is so that both practitioners and researchers can be clear about what they are discussing. Although different interpretations can add richness to understanding a concept, they can also lead to confusion and ambiguity. A review of the definitions and functions of ISPs revealed that the term is not used consistently across authors. There are also distinctions between technical and managerial policies and between policy architecture and documents included in the term.

A surprising observation can be made from the statements of definitions and functions of ISPs. Many articles explain that the purpose of an ISP is to "facilitate the prevention, detection, and response to security incidents" (Cram et al., 2017, p. 605). While there is no reason to dispute this definition, it overlooks the obvious reasons for IS. Apart from organizations that are in the business of secrecy, the *raison d'être* for most organizations is to achieve completely other objectives than security. IS threats stem from the operating environment, and the organization merely tries to cope with them using ISPs. It seems that there is a need for definitions and research approaches that shift the focus from IS as the objective to IS as an enabler for business objectives. If IS is developed for the sake of security and not to enable the organization to operate, it may lead to executing measures that are unnecessary and even unwanted.

There is no single description of what an ISP comprises, and that is why ISPs may be significantly different from organization to organization. This literature analysis revealed many descriptions and functions for ISPs. However, we also detected many background assumptions of the definitions that were not explicitly expressed. Here, distinctions were made between the description and function of an ISP, even though many authors have mixed these notions. What the ISP is must adequately support what it does. For example, if stated rules are insufficient or imprecise, it cannot be expected that every employee would interpret them in the same manner. Further, we cannot presume that the existence of any characteristic of a policy would inevitably lead to any of its functions. For example, the mere existence of predefined sanctions may not lead to compliance (Siponen et al., 2022). A deeper understanding of the definitions and functions of ISPs may help in widening the view of the nature of the policy in development.

There is a need to explain what definition of ISP is used here to form a mutual understanding with the reader about the subject of this thesis. The following points are a choice made for this thesis based on the literature and their usefulness in the upcoming empirical study.

An ISP:

- is a formalized description of how the organization addresses IS,
- is created to steer the use of an organization's information assets,
- is specific to the organization and plays a part in reaching the organization's goals,
- is stated in a way that concerns the entire organization (sub-policies may cover only some parts of it),
- includes rules that organization members are expected to follow, and
- has several abstraction levels, from high-level goals to practical guidance.

2.2 ISP development methods

Both research and practitioner literature have introduced a number of different approaches for ISP development. ISP development methods have become more complex over the years, as have the systems and organizations they are protecting. Baskerville (1993) studied the evolution of security design methods using characteristics that can be identified in general information system design methods. He noted that security design methods lag behind the general methods and are moving towards understanding the increasing diversity of security needs in these systems (Baskerville, 1993). A similar increase in complexity can be identified in ISP and security management methodologies (Klaic, 2010).

There are multiple approaches to ISP development, but selecting the right one for the organization may be difficult. A method has been created for choosing the right IS strategy approach where a business falls into one of four types (low/high perception of risk, and use of IT being operational tool/competitive advantage) (McFadzean et al., 2007). Decisions on IS strategy further affects the development of IS governance and policies. Saleh (2011) created an IS maturity model with five levels of compliance, that can be used to assess an organization's capabilities to meet security goals.

Since ISPs affect the organization (as do any other policies), it is often recommended that the ISP lifecycle should be connected to other existing processes (Baskerville & Siponen, 2002; D'Aubeterre et al., 2008; Galletta & Hufnagel, 1992; Posthumus & von Solms, 2004). Connecting the ISP lifecycle into general management and strategic processes has become an increasingly popular approach (Klaic, 2010). An ISP can be one of the policies developed within the strategic management cycle (Corpuz 2011). The alignment of processes can be undertaken at all levels, from strategic to operational. One approach to highlight information flows and security concerns in operational-level business processes is via modeling languages, such as secure activity resource coordination and the enriched-use case (D'Aubeterre et al., 2008).

The ISP architecture (ISPA) by von Solms et al. (2011) suggests that ISPs should be created by starting from high-level statements and then moving to more detailed policies. Strategic-level policies are created first at the highest level of the organization, and then they are expanded or disseminated to tactical and operational levels as more detailed policies. The ISPA was created due to the observation that operational-level policies were not always in line with higher-level policies, as they were created by the staff to support daily operations (R. von Solms et al., 2011). Coles-Kemp (2009) argued that these kinds of informal power structures that shape the ISPs are not sufficiently acknowledged in the IS literature. Lapke and Dhillon (2008) created a method to map power relationships in the organization to choose the right people to participate in policy development.

Selecting the rules for an automated policy can be straightforward since they generally do not allow for the user's judgment regarding whether or not following the policy is prudent. Security logic is an example of a language designed to describe these policies (Glasgow et al., 1992). The earlier generations of managerial ISP development were similarly simpler due to the variety of information and communications technology (ICT) solutions being smaller and views on the human factor receiving less attention. For example, Wood (1995) proposed that policies should be developed by gathering reference materials, deciding on a framework, and preparing a coverage matrix. The coverage matrix is then used to check for the coverage of policies between control categories and audiences. This method can be seen as an example of Siponen's (2005) argument that traditional security methods tend to reuse some underlying assumptions, such as control orientation.

The literature provides simple models for general ISP development as well as specific methods for parts of the process, such as choosing the right people (Lapke & Dhillon, 2008) and identifying information (D'Aubeterre et al., 2008). The connection between the contextual factors, content, and method is acknowledged, but in many cases, it is not supported in the description of the method on a practical level. The following section further analyzes existing ISP development methods.

2.2.1 ISP development lifecycles

Over the years, several different approaches to ISP development have been proposed. A common practice is that the ISP development process is connected to a lifecycle model. This view is commonly accepted and described in numerous textbooks, with recommendations for responsible personnel, phases, and outcomes (Howard, 2002; Raggard, 2010, p. 52). A comparison between some exemplar ISP development lifecycles is depicted in FIGURE 1. These models are process-level representations of the entire ISP lifecycle. The different phases in the models have been presented as linear processes to highlight the similarities between the models. However, many of these original models recommend iterations in one or multiple phases. The phases have also been aligned with other models in the illustration to highlight the similarities and differences before, during, and after ISP development.

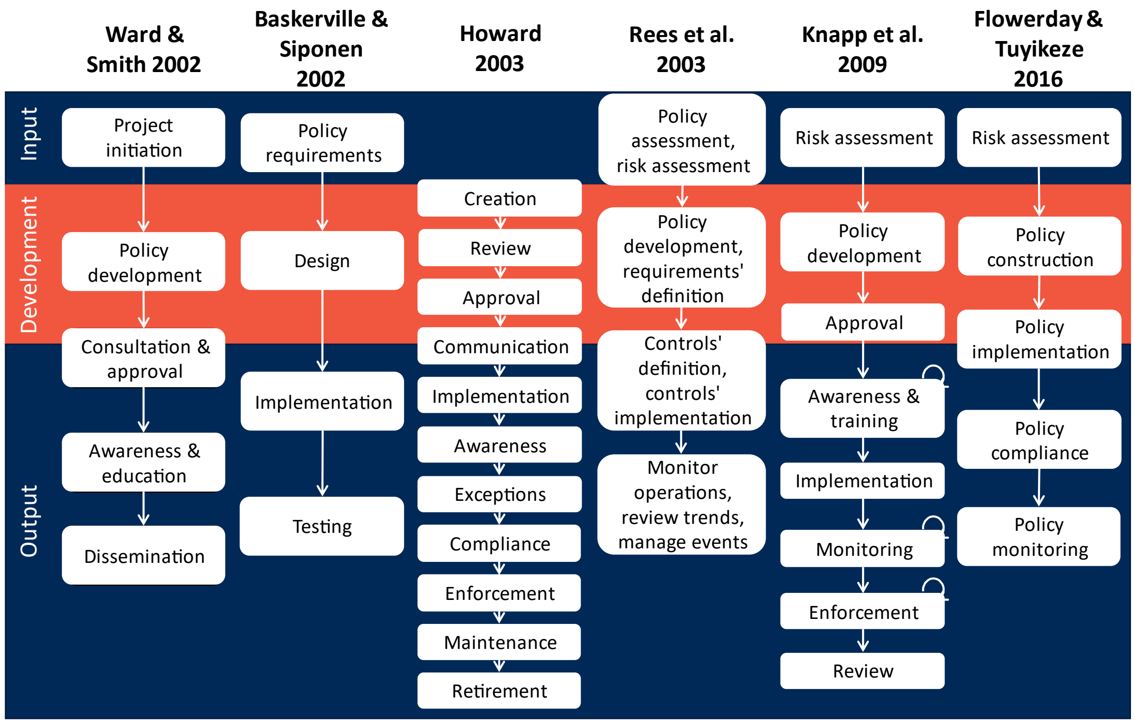


FIGURE 1 ISP development lifecycles

Ward and Smith (2002) describe the development of an access control policy in five distinct phases. This developmental method does not prescribe the input and analysis of raw data but describes the processing and outputs of the policy in detail. The input to the ISP development process is described only as the project's initiation. Risk and requirements assessment are stated to be important but not described further. Other phases in the method include policy development, consultation, awareness, and dissemination. (Ward & Smith, 2002.)

One major problem with stating general "one-size-fits-all" policy development methods is the different characteristics and environments that organizations have (Baskerville, 1993). Baskerville and Siponen (2002) an IS meta-policy for emergent organizations to support meeting organization-specific requirements in ISP development. Within this approach, the main requirements for creating a policy are the identification and classification of policy subjects and objects. Then, the design process determines the architecture and scope of the policies. Finally, the policy is implemented and tested. The authors argue that following through with this strategic approach to an ISP would assist in tailoring the policy to the organization in question. This approach is particularly designed for emergent organizations that must have mechanisms in place to update their ISPs whenever the organizations face changes. (Baskerville & Siponen, 2002.)

Howard (2002) described the security policy lifecycle through 11 functions creation, review, approval, communication, implementation, awareness, exceptions, compliance, enforcement, maintenance, and retirement. The creation function contains many separate components that involve gathering, analyzing, and creating data simultaneously. This model is more detailed in describing phases than some of the other models. For example, approval, communication, and implementation are here described separately, while in some other models, they are all under implementation. (Howard, 2003.)

The Policy Framework for Interpreting Risk in e-Business Security (PFIRES) was created to support organizations that need to adapt to frequent changes in software while aligning the ISP with the organizational requirements (Rees et al., 2003). This tool is cyclical in nature and consists of four phases (assess, plan, deliver, and operate), which all contain two sub-steps. This framework provides practical descriptions of the tasks in the input, development, and implementation phases, but the method does not consider long-term maintenance issues, nor does it discuss how the inputs to the process are analyzed. (Rees et al., 2003.) The PFRIES has been critiqued for lacking support for translating policy recommendations into requirements (Antón & Earp, 2001).

Knapp et al. (2009) created an organization-level process model based on a qualitative survey of IS professionals. A distinctive feature of this model is that it considers stakeholders outside the ISP development team and includes internal and external influencing factors. This model also depicts several iterations within and between phases to reflect the practices reported by the professionals. The first iteration circle includes risk assessment, policy development, and policy review. After the policy content is set, the cycle moves on to approval, awareness and training, implementation, monitoring, enforcement, and back to review. This model also includes the retirement of policy, audits, and automated monitoring tools. (Knapp et al., 2009.)

Another broad-reaching approach to ISP development was prescribed in the ISP development model (Flowerday & Tuyikeze, 2016). The steps in this model are based on literature analysis (Tuyikeze & Flowerday, 2014), and the created constructs were tested by surveying professionals. Like in many other models, the risk assessment provides the primary input to the ISP development. This is followed by policy construction, policy implementation, policy compliance, and policy monitoring. The model also describes additional inputs and motivations into the process, including security policy guidance, security policy drivers, existing theories, management support, and employee support. The practices for implementing the method or additional inputs are not discussed further than naming the stakeholders who are to be included in the process. (Flowerday & Tuyikeze, 2016.)

The lifecycle models discussed here are portrayed as simplified versions in FIGURE 1 to enable comparison. The steps in the models have been matched with the general phases of ISP development inputs, development, and outputs. In the following sections, the development process is considered to consist of all the steps of the process that include creating or changing the content of the ISP. Inputs and outputs include other steps or processes linked to ISP development.

2.2.2 Inputs to development

The ISP development process needs inputs before it can start. An initial decision must be made to start ISP development, people need to be appointed to the job, and some actions can be undertaken to analyze the current state of the organization, its operating environment, and IS (Knapp et al., 2009; Ward & Smith, 2002).

The facts of the organization and the state of security within that organization should inform the planning phase of ISP development. There are three factors that have been identified to influence ISP design: standards and regulations, the desired format, and internal and external risks (Cram et al., 2017). Knowledge gathering and analysis are here considered inputs and thus separate from ISP formulation. In reality, knowledge gathering, and policy development may also occur simultaneously in a rapid feedback loop (Knapp et al., 2009).

Trček (2003) offered a framework for IS security management and policy formulation. As it is related to the entire process of security management, a security policy is only part of the entire framework. For the formulation of a security policy, this framework suggests adhering to British standard BS7799 (Trček, 2003), which is now incorporated in ISO/IEC27002 (Hsu, 2009; Siponen & Willison, 2009). In this standard, policy development is described through an input–process–output model. The “input” includes reviewing the legislation, contractual obligations, standards, and requirements. The “process” of the framework includes analyzing the security organization, the control and assets, physical and environmental security, personnel security, access control, and compliance. Regarding the “process,” the basic criticism of the ISO IS management standard is that it does not explain the content or quality of the process (Siponen, 2006). To be more precise, such standards require organizations to have an ISP but do not explicate a process or the characteristics of how one develops a good-quality ISP.

Trček's (2003) framework, along with many others (e.g., Burgemeestre et al., 2013; Cram et al., 2017; Whitman, 2008), calls for the use of standards and legislation as inputs for ISP development. Common examples of laws affecting the formulation of ISPs are the Sarbanes–Oxley and Health Insurance Portability and Accountability Act in the United States and the General Data Protection Regulation (GDPR) in the European Union (EU). Many organizations are bound to adhere to other laws and regulations as well that are specific to their field of operation, and these may affect the design of the ISP. Some standards may support the development of an ISP that also complies with the law (Haworth & Pietron, 2006). However, in many cases, the burden of fitting the two sets of external requirements together falls on the organization (Burgemeestre et al., 2013).

While using predefined requirements can help in creating inputs to ISP development, many scholars warn against relying on them too much (Baskerville, 1993; Cram et al., 2017; Dhillon & Backhouse, 2001; Hedström et al., 2011; Siponen & Willison, 2009). These approaches often rely on identifying persistent general risks but may overlook organization-specific threats that are specifically targeted at the organization by exploiting its weaknesses (Baskerville et al., 2014). Some researchers have also noted that certification for these standards may shift the objective of the ISP development effort from preparing against IS threats to mere compliance (Hsu, 2009; Siponen, 2006).

In addition to external requirements for an ISP, many areas within the organization generate requirements for security. The security logic framework provides a higher-level perspective on how a security analyst gathers information about the state of security within an organization. It defines what a subject knows, what information a subject has permission to know, and what information a subject is obligated to know. As it is user-centered, the often-missing human element can get the focus it needs to ensure an effective security policy (Glasgow et al., 1992). This call for user-focused requirement gathering was also noted by Baskerville and Siponen (2002), who described two essential requirements that should be considered when planning a security policy: the identification of security subjects and objects and the classification of security subjects and objects.

The ISP lifecycle models in FIGURE 1 recommend requirements gathering or requirements assessment before the design phase. The cyclical frameworks (Knapp et al., 2009; Rees et al., 2003) acknowledge that there may be a previous policy that can be assessed in light of compliance, security incidents, and emerging requirements. Monitoring the previous policy is advised to provide a way to receive signals for the need for a new development cycle (Rees et al., 2003). The frameworks also recommend a risk assessment. Depending on the assessment instrument in use, this may involve identifying threats, evaluating assets, and identifying business requirements from an IS standpoint (Flowerday

& Tuyikeze, 2016; Rees et al., 2003). Risk assessment is a research area, both in IS and business management, which has produced many different approaches for risk evaluation (Baskerville, 1991).

The approaches to ISP development methods have evolved over the past decades. Baskerville (1993) created a taxonomy of three generations of IS security design methods that included: checklists, mechanistic engineering methods, and logical-transformational methods. Siponen (2005) continued this work by comparing the underlying assumptions of the major IS security methods: checklists, standards, maturity criteria, risk management, and formal methods. In this comparison, the methods prescribed by the practitioner-oriented papers fell into the first two generations. For example, the "security principles" proposed for the health field (Anderson, 1996; Gritzalis, 1997) imply a generic checklist (1st-generation IS security methods). Using standards as a critical form of input (Trček, 2003) typifies a 2nd-generation IS security method. Understanding the evolution of recommended inputs to ISP development contrasts with the current trends that advocate a more versatile and detailed view of inputs.

2.2.3 ISP development

In the ISP development process, the inputs are turned into the output of the completed policy. The design of the ISP can include the policy architecture (Baskerville & Siponen, 2002; R. von Solms et al., 2011), determining abstraction levels (Baskerville & Siponen, 2002), language format (Goel & Chengalur-Smith, 2010), and document format (Baskerville & Siponen, 2002). This area of IS development is widely covered in the best practice literature (such as standards) but lacks research in some areas. In particular, articles that provide research data from the field to support recommendations for working methods or design choices are scarce.

The ISP development may begin by analyzing the inputs and making design choices. The developers may use a general list of topics or decide on a policy architecture (Baskerville & Siponen, 2002; Finnish Standards Association, 2014; R. von Solms et al., 2011). The concept of designing a policy based on the flow of information from the inputs has been mentioned in many articles, but the mechanisms for how to do this are rarely discussed in detail.

Different parts of the policy architecture may need different development teams (R. von Solms et al., 2011). Strategic-level policies may require input from the top management who created the business strategy, while different business units, such as IT or human resources, may develop lower-level operational policies (Rees et al., 2003). The organization members may be supported by consultants (Gritzalis, 1997). The ISP developers should have a comprehensive view of the operations of the company. For example, the IT department rarely has this knowledge, and their efforts alone may lead to an ISP that focuses on technology, omitting other aspects of IS (Knapp et al., 2009; Maynard et al., 2011).

The ISP documentation is a medium of communication, and thus choosing the suitable format for the policy is not a trivial task. It is often advised that the policy document should include definitions of key concepts (Höne & Eloff, 2002; Trček, 2003) since the developers of the policy and the readers may understand these concepts differently (Hedström et al., 2011). Keeping the text short and to the point has been shown to be more effective in communicating the policy (Goel & Chengalur-Smith, 2010).

Before the ISP may be deemed ready to move to implementation, it may need to go through an approval process. First, it is recommended that the development group try to reach a consensus and that the person responsible for IS in the organization approve the final version (Lindup, 1995). Different business areas can also be asked to review the content to reduce ambiguity and difficulties in implementation (Talbot & Woodward, 2009). In many ISP development methods, it is advised that approval is formally sought from top management (Flowerday & Tuyikeze, 2016; Höne & Eloff, 2002). It has been noted that if management does not have expressed commitment to the goals of the ISP, it may not get the time and attention it requires (Talbot & Woodward, 2009), which leads to the organization operating in an unsecure manner (Höne & Eloff, 2002). Approval from the top management gives a credible mandate to implement the ISP and demand compliance (Höne & Eloff, 2002; Soomro et al., 2016; Wood, 1995).

Baskerville and Siponen (2002) have recommended testing the new ISP before implementation. The tests should reveal if the policy meets the IS requirements, matches the design, and indicate possible problems in the implementation phase, such as new threats (Baskerville & Siponen, 2002; Rees et al., 2003). Pilot testing (Rees et al., 2003) and testing contingency plans in "real" situations (McFadzean et al., 2007) have also been recommended. Usually, in lifecycle models, the testing phase comes after acceptance and implementation. However, since testing may still result in changes to the ISP, it should be considered a part of development efforts.

Trompeter and Eloff (2001) provided a framework for the implementation of socio-ethical controls in IS security. Socio-ethical controls are defined as "the conforming of an organization to recognized information security ethical principles" (Trompeter & Eloff, 2001, p. 386). The core argument was that people should be placed at the center of the equation rather than at its periphery. One way to do this is to "adopt an information security policy that includes its viewpoint on socio-ethical IS security awareness issues. This policy can then be used to guide staff members in the various ways in which to protect client information" (Trompeter & Eloff, 2001, p. 387). This framework instantiates later generations of IS security methods (Baskerville, 1993; Siponen, 2005).

In this section the ISP development process was limited to only include tasks that create or change the policy. After the ISP is ready, it moves to the implementation phase. However, if the implementation process is considered to include developing sub-policies or guidelines, it would make this phase a part of development efforts (Abrams & Bailey, 1995). Similarly, if the implementation includes testing, which may lead to changes in the content, then it is still a part of the development process. Testing can also happen after implementation, and, in this situation, it functions as a tool to detect the need for a new development cycle (Olnes, 1994).

2.2.4 ISP development in practice

The bulk of the ISP development literature depicts the process at a general process level. There are many prescriptions of what should be done but not many descriptions of how the method is acted out in practice. However, there are some published studies with rich qualitative data that shed light on the realities of the endeavor. The actual practice of ISP creation is often messy, full of conflicts, incomplete, and does not follow the development methods perfectly (E. Niemimaa, 2016a).

A practice lens has been used to describe messiness in information classification policy development (E. Niemimaa, 2016b; E. Niemimaa & Niemimaa, 2017). An ethnographic study revealed that instead of moving through the stages of assessment, development, and implementation neatly, the IS manager had to go through the stages of formulating the policy and collecting feedback three times before the information classification scheme was accepted by the work community (E. Niemimaa, 2016b). The study highlighted the fact that ISP development methods often provide very little advice on the actual work needed for the higher-level steps, such as how to adopt policy formulation for different practices and actors. The authors recommend that researchers and practitioners focus more on issues related to the transformation from general guidelines to local practices (E. Niemimaa & Niemimaa, 2017).

Karlsson et al. (2017) assessed ISPs from a practice perspective with data from healthcare professionals. They claimed that ISP documents cannot be studied without considering the practices that generate these documents. They present eight tentative quality criteria for ISPs, which include aligning the policy statements to work practices, structuring the documentation with the employee in mind, and declaring policy subjects and their responsibilities unambiguously (Karlsson et al., 2017.).

Burgemeestre et al. (2013) studied the dialogues and trade-offs that were made during a security evaluation. The goal was to shed light on the reasoning behind security decisions so that they could be more easily communicated to, for example, an external auditor. Based on a value-based argumentation scheme, critical questions were used to challenge the justifications behind the decisions. These questions could challenge the usefulness of a control in a certain situation, for example, if the measure creates undesired side effects or if the measure does not support the values the organization wants to pursue. (Burgemeestre et al., 2013.)

When we move away from the expectations that the prescribed ISP development methods create and try to see how things are done in real life, we can better understand how different practices lead to different outcomes. In these practice-level studies, the focus is often an attempt to illustrate how including employees in the ISP development process leads to rules that better fit the daily operations of the organization. User involvement is expected to positively affect security endeavors as they utilize users' know-how and create buy-in (Albrechtsen, 2007).

2.2.5 Outputs of development

The output of a development project is the ISP and its documentation. The ISP lifecycle models name phases after the policy development, such as implementation, maintenance, enforcement, and monitoring (FIGURE 1). With technical ISPs, implementation is the process of putting a system into use and can include areas such as coding, off-the-shelf purchases, outsourcing, testing, and user training (Abrams & Bailey, 1995; Anderson, 1996; Wood, 1995). Within managerial ISPs, this phase primarily refers to applying the policy within the organization by guiding and training the employees (Heikka, 2008; Hsu, 2009; Tuyikeze & Flowerday, 2014). A large portion of the ISP literature considers this phase of the policy lifecycle from the viewpoint of awareness, security culture, compliance, and reaching security objectives (Cram et al., 2017).

A study by Doherty and Fulford (2005) found that there was no statistically significant relationship between implementing ISPs and the incidence of security breaches. This may seem detrimental to the core assumption of the usefulness of security policies, but it can also be considered to make a case for focusing on quality in ISP development. The authors suggested that difficulties in raising awareness and enforcement, overly complex policy standards, inadequate resourcing, or the failure to tailor policies for the organization might be the reasons behind the ineffectiveness of the ISP (Doherty & Fulford, 2005). This highlights the importance of user training (Heikka, 2008) and testing (Baskerville & Siponen, 2002). Activities involving user participation are important when trying to change security behavior (Albrechtsen, 2007; Siponen & Puhakainen, 2010; Karjalainen & Siponen, 2011).

ISP compliance can be addressed before full-scale implementation. Lapke and Dhillon (2008) analyzed resistance to security policies through the lens of power relationships. In a case study, they found that although there was a well-documented and planned set of processes in place for the formulation and implementation of security policies, the implementation efforts failed to explicitly acknowledge the effects of resistance and implicit power brokers. The authors recommend that the people responsible for policy formulation should perform an extensive analysis of the impact an ISP might have on productivity prior to implementation. (Lapke & Dhillon, 2008.) Siponen (2000, 2001) argued that resistance to ISPs may also arise from a person seeing certain actions as totally wrong or deficient and that policymakers should be ready to justify their choices for the guidelines if challenged. These studies imply that measures undertaken during ISP development, as well as during user training and testing, could suppress some of the resistance during implementation. If the organization members do not understand the nature and importance of an ISP, it may hinder its adoption altogether (Lopes & Sá-Soares, 2010).

In cyclical ISP lifecycle models, the output of the development phase returns later as an input to a new ISP development or revision process. The reasons for a new iteration in the development cycle may be changes in the business environment, new technological solutions, or a failure to reach the security objectives of the ISP (Baskerville & Siponen, 2002; Rees et al., 2003). Detecting changes and reaching goals can be achieved by monitoring predetermined metrics that can be built to match the policy architecture (R. von Solms et al., 2011).

2.2.6 Overview of the methods

ISP development methods are often presented as lifecycle models, but usually, only one phase of the model is responsible for creating new content for an ISP. This literature analysis focused on this phase, and the previous and consecutive phases are called the inputs and outputs.

The literature recommended ISP development inputs such as standards, regulations, the desired format, risk analysis, contractual obligations, user-related requirements, previous policies, logs of security incidents, and business requirements. However, using predefined focus areas for assessing the starting point of the ISP development may be problematic. When applying general advice to specific contexts, it may leave blind spots and create a false sense of security. They may turn the development process into something that focuses on replicating processes rather than focusing on IS and the organization-members needs and preferences (Ashenden, 2008; Siponen, 2006).

The literature promotes the use of certain inputs to the ISP development process, such as risk assessments or standards. However, there is not much advice available explaining how these inputs are successfully turned into policy statements. Few authors have provided special techniques for making choices in the development phase, such as methods for solving value conflicts (Burgemeestre et al., 2013; Hedström et al., 2011). While there are many calls for, for example, management and user participation (Ashenden, 2008; McFadzean et al., 2007; M. Niemimaa & Niemimaa, 2019), meeting organization-specific requirements (Baskerville & Siponen, 2002), and assuring quality documentation (Cram et al., 2017; Goel & Chengalur-Smith, 2010), there are very few research-based recommendations on how to do these things well.

The recommendations for involving organization members in the ISP development stem from the research on ISP implementation and compliance. One popular topic is determining the causative effects on policy subjects' awareness or acceptance of the ISP to policy compliance (Cram et al., 2017). Another approach is the research on power relationships (Lapke & Dhillon, 2008) that has found that the possible conflicts that arise from the change in power relationships can be reduced by better design of the ISP in the first place. However, we know little about what kind of effect does including organization members have on the content of the ISP or its performance after implementation.

The quality of the ISP development outputs can be evaluated after implementation. In ISP lifecycle models, the detected issues with the policy may be a reason to start the cycle from the beginning. Other reasons for starting a new cycle can be a predetermined lifespan for the ISP or changes in the organization, such as a new strategy, if the ISP process is tied to the strategic planning process (McFadzean et al., 2007). The research literature gives very little advice on the proper ways to detect a suitable time for ISP revision. Without a plan for ISP revisions, changes could be made only when security incidents occur and cause harm. It is advised to include the creation of performance metrics during ISP development to avoid ad hoc changes made in a state of panic (Baskerville & Siponen, 2002; Burgemeestre et al., 2013).

2.3 Organization-specific aspects of ISP development

ISP development methods are, to a large extent, general instructions aimed to suit all or certain types of organizations. Research on the topic has also yielded recommendations on how to adapt these methods to specific organizations. Next, we will take a closer look at the specifics of ISP development, mainly ISP content, ISP context, and alignment with organizational goals. Lastly, different abstraction levels of ISP development research are discussed.

2.3.1 Content of the ISP

The aim of ISP development is to produce a documented policy, but the form of the documentation may vary greatly across organizations. It might be a massive manual covering everything, many shorter hierarchically connected policies, or a one-page high-level policy statement supplemented by guidelines. An example of a hierarchical policy structure is provided in the ISPA, which has strategic-, tactical-, and operational-level policies (R. von Solms et al., 2011). Policies may also be area-specific, or they may be targeted at different users (Doherty et al., 2009). Sterne (1991) stated that technical automated security policies and managerial policies governing human behavior should be separate documents that are linked together.

A classic definition of the ISP is to protect the confidentiality, integrity, and availability (assurance of the service) of information, but this view has been criticized for its strong focus on technical security (Sterne, 1991). Therefore, equal attention needs to be given to both technical and managerial policies. They should not solely focus on listing controls but also explain the reasoning behind them to make it clear to both the developers and the readers, why these controls exist. For example, a study in a healthcare facility found that the staff considered strict privacy rules to apply only to digital patient records, but not to the paper files that were also used (Hedström et al., 2011).

The analysis of definitions (see Section 2.1) revealed that there are various views on the nature of ISP content. Some authors promote a rule-oriented view, which incorporates sanctions based on deterrence theory (Siponen et al., 2022; Straub, 1990) while others suggest guidelines that allow users to make security decisions in new situations. Siponen and Iivari (2006) investigated how ISP design could be explained through normative theories from philosophy. They argue that all-inclusive and strict policies fit organizations where exceptional situations are uncommon, and the subjects are not expected to make security decisions. However, if an organization operates in a volatile environment and trusts its employees to make decisions, then more general guidelines may yield better results. (Siponen & Iivari, 2006.) In addition, the enforcement tactics stated in the policy may vary from punishing incorrect behavior to rewarding good deeds, depending on the organization (Chen et al., 2012).

ISP content may be created on the basis of IS management standards, such as ISO27002 or regulations, such as EU GDPR. In some cases, following a standard helps in complying with regulations as well (Haworth & Pietron, 2006). However, Höne and Eloff (2002) examined several standards and noticed that they focused more on the processes of implementing the ISP rather than on providing guidance for the development of its content. Further, it has been noted that general guidelines for policy content seem to provide more support for creating preventive controls than responsive ones. Incidence prevention is possible when risks and their countermeasures are known. If the organization operates in an environment where new risks constantly arise, they need a policy that supports responsive actions. (Baskerville et al., 2014.)

ISP literature also provides special guidance for certain industries. For example, Anderson (1996) and Gritzalis (1997) presented principles to guide the formulation of ISPs in medical facilities, with a special focus on the privacy of patient information. Anderson's (1996) principles cover access control of patient records, while Gritzalis's (1997) principles guide a more comprehensive security program. However, these general principles may not suit all healthcare units depending on local legislation and values. Therefore, the rules on the secure use of patient records should be negotiated locally (Hedström et al., 2011).

It should not be assumed that a single organization needs a single ISP. Organizations and their information systems may not form a cohesive whole but instead, consist of different units that use vastly different information assets. Lindup (1995) recommended a security treaty to be used where a comprehensive ISP is not possible. It suits organizations that comprise of several independent units, and it highlights the individual needs and common goals of these units. Additionally, Ward and Smith (2002) proposed a set of eight indicative policies for organizations with distributed systems.

As there are many ways to construct the general structure of the ISP content, there are also many ways to write the actual policy text. Goel and Chengalur-Smith (2010) created metrics for policy document breadth, clarity, and brevity. They suggested that these attributes may influence policy subjects' ability to comprehend the document, which would lead to better compliance and IS. An example of this is provided by Albrechtsen (2007), who found that employees would not spend time reading documentation that they considered too long and complex. Ultimately, the documentation of the ISP should match the communication culture of the organization.

2.3.2 The context in ISP development

As was argued in the section on ISP content, creating policies that would suit all companies is hard or even impossible, as the context of the policy affects what kinds of rules can be applied in different organizations. General guidelines can only direct toward assessing the context but cannot provide universal answers. They cannot address organization-specific IS needs or detect blind spots (Siponen & Willison, 2009).

While context is something that is quite unique for each organization, research has tried to find commonalities across organizations. Karyda et al. (2005) analyzed two case studies and identified seven contextual factors that influence the formulation and implementation of ISPs: "organizational structure, organizational culture, management support, contribution to users' goals, security officers, users' participation in the formulation process, and training and education" (Karyda et al., 2005, p. 268). Shortcomings in these factors, such as organization culture that ignores security concerns, could be seen as reasons to start developing or revising the ISP (Talbot & Woodward, 2009).

Galletta and Hufnagel (1992) created an end-user compliance model in which the context affects both the content and the policy development process and, eventually, compliance. The research to validate their model was unable to prove that compliance resulted from the context-specific design of the policy or from users' personal inclinations to follow the rules. Later, it was shown that a person's attitude, perception of control, and subjective norms do affect the intention to share knowledge about IS (Safa & von Solms, 2016) and thus contribute to the security culture of the organization.

Da Veiga and Eloff (2010) created a framework and assessment instrument for an IS culture to evaluate the cultural changes related to security measures. They noted that the security culture could also affect security measures, such as ISPs, and suggested user participation in the development process, especially in individualistic organizations. Insiders have been deemed one of the largest risks for IS, since they have access to the information assets and can unintentionally or maliciously use them in an undesirable way (Colwill, 2009), which is why many authors emphasize their role.

Managers play an important role in the development and implementation of the ISP. They can contribute to many context-related issues, such as the alignment of IS and business processes (Soomro et al., 2016). However, many approaches to IS management expect that the company structure reflects the distribution of power and authority and that decisions can always be made through a formal process which is not always the case (Coles-Kemp, 2009). ISP development can be improved if the local power structures are identified and key persons are involved (Lapke & Dhillon, 2008).

The ISP development process may include several stakeholder groups, such as "business unit representatives, executive management, human resources, ICT specialists, security specialists, legal & regulatory, public relations, user community, and external representatives" (Maynard et al., 2011, p. 187). Stakeholders have their own views on IS, and they have different metaphors and terminology to describe the same information-processing tasks (Abrams & Bailey, 1995). Stakeholder participation can create buy-in, a sense of democracy, and turn them into advocates for the policy, which is later beneficial in the implementation phase (Maynard et al., 2011; M. Niemimaa & Niemimaa, 2019; Rees et al., 2003). It must also be noted that the person's role in the organization is not the only thing that affects their security behavior; their individual personality and aspirations also affect it (Ashenden, 2008).

Since ISPs contain descriptions of desired and undesired actions, they can be seen as reflections of values. Different stakeholders can have different values, which raises the question of whose values the ISP serves (Siponen, 2000). A value-based argumentation method for ISP development has been proposed to solve conflicts between, for example, business interests and regulations (Burgemeestre et al., 2013). The value-based compliance model tackles the same problem by seeing users' noncompliance as a rational action due to their different values, which conflict with the ISP (Hedström et al., 2011). For example, healthcare staff may prioritize patient safety and keeping appointment schedules before ISP compliance. This is in line with the finding that people who are open to changing their values may act against policies, whereas those who do not make higher-level decisions about their values and only try to avoid sanctions will follow policies (Myyry et al., 2009).

The organizational context of the ISP can affect both the content and the development method of the policy. Context refers not only to the externally identifiable characteristics of the organization, such as process charts and competitors, but also to policy subjects' inner characteristics and social dynamics. At a higher level, the policy should meet the security requirements and business objectives of a specific organization (Karyda et al., 2005). At an individual level, the policy should allow the subjects to perform their duties without conflicts with other responsibilities or values (Hedström et al., 2011). Disregarding the context while developing the policy may lead to failure during implementation and non-compliance (Chen et al., 2012; Hsu, 2009).

2.3.3 Alignment of ISP with organizational goals

Business policies, including ISPs, support organizations' efforts to reach their goals, and the ISP should be aligned with these goals (Antón & Earp, 2001; Höne & Eloff, 2002). Connecting ISP development in the strategic management cycle could ensure that the alignment between business and IS goals is constant, even when the organization's goals change (Corpuz, 2011). If the business strategy is not included in the ISP development inputs, it may lead to high-risk assets that are not strategically relevant being overly protected, or vice versa (Burgemeestre et al., 2013). When it is clear that the ISP is designed to contribute to the strategic goals, it can also be easier to justify the investments made in security (Klaic, 2010).

Many ISP development methods suggest ways to include the business strategy in the policy, such as involving senior management (Flowerday & Tuyikeze, 2016; Knapp et al., 2009). von Solms et al. (2011) suggested that the management direction of IS should start from the strategic management level, and the tactical- and operational-level policies should be directly derived from the high-level policies. Business directors' perceptions of risk and the role of IT influence how they direct the planning, adoption, and use of IS measures (McFadzean et al., 2007). Analyzing these perceptions of risk and IT can be used in creating an IS strategy by mapping the current situation, identifying contextual factors that influence the strategy, and setting future goals. Most importantly, the analysis helps align the IS strategy with the business strategy (McfFadzean et al., 2007). By understanding the types of risks and the strategic need for IS, it is possible to move on to making decisions about choosing the right mix of prevention and response strategies for that specific type of business (Baskerville et al., 2014).

One notable drawback in many strategy-ISP alignment recommendations is the expectation of a large corporation. However, small- and medium-sized enterprises (SMEs) are a vital part of the economy, but there is less support available that would fit their needs. SMEs are often characterized by limited financial or human resources, a low level of formalization in the organizational structure, an insulated operational environment, and a lack of a strategic outlook (Heidt et al., 2019). These characteristics can constrain an organization's ability to detect the need for IS and its capability to respond to it (Yildirim et al., 2011).

The role of IS is to enable an organization to operate and reach its goals. It is possible to derive the goals of the ISP from the business goals of the organization. However, without proper planning and a methodological approach, alignment may easily fail or be omitted, and this can lead to the dual development of business and IS goals.

2.3.4 Addressing organizations' needs at all levels

Adopting an ISP that meets the organization's needs should be at the core of any advice given about the matter. Many IS recommendations rely on the fact that global IS threats, such as ransomware or denial-of-service attacks, could happen to anyone using connected devices. While there is no disputing this, it must be kept in mind that the repercussions of these risks and the efforts needed to mitigate them vary greatly across organizations. Therefore, the key question is not what threats there are; instead, it is what the organization needs to do despite these threats. The answer is not simple and must be addressed at several different levels of planning and execution.

Similar to what von Solms et al. (2011) described about the abstraction levels of ISP architecture, the research on ISP development can be viewed through different levels of abstraction. The highest level is research that considers how IS processes link to other functions of the organization or compares types of organizations. Questions about strategy alignment and IS management styles could be positioned at this level. The unit of study at this level is the entire organization or its units. The middle level of ISP research considers the process level and is best represented in the current ISP development literature. Cyclical process models, where the actual ISP development is only one part of the entire ISP lifecycle, are located on this level (see examples in FIGURE 1). At this level, the unit of study is the overall work processes in IS management. The lowest level of abstraction considers the actual practices and situational considerations of ISP development. The unit of study is individuals and social interactions. Examples and a comparison of these abstraction levels is provided in TABLE 2.

TABLE 2 Examples of different abstraction levels in ISP research

Abstraction level	**Research problem**	**Unit of study**
High	"we describe the necessary shift from a prevention-centered security framework to an alternative, broader information security management framework [that] focuses on the balance between prevention and response" (Baskerville et al., 2014, p. 139) "explore how boards perceive information security and how this perception influences their own actions as well as the development, adoption and use of their information security strategy." (McFadzean et al., 2007, p. 623)	Comparison of organizations' strategies
Medium	"development of a practice-based organizational model describing a comprehensive security policy process" (Knapp et al., 2009, p. 494) "proposal of a key component "1" in the framework termed the "Information Security Policy Development Life Cycle" […] This framework indicates the various constructs that information security practitioners need to consider in the development and implementation of an effective [ISP]." (Flowerday & Tuyikeze, 2016, p. 169)	Process steps and influencers
Low	"Drawing upon the value-based compliance model, we propose a new technique for mapping complex security situations in an organization." (Hedström et al., 2011, p. 374) "How do organisations develop InfoSec policies that are sensitive to employees' work practices and organisational contingencies but also align with the technical expert knowledge contained in InfoSec best practices?" (M. Niemimaa & Niemimaa, 2019, p. 2)	Work practices and individual rules

A significant drawback in the ISP literature is the disconnection between different levels of abstraction. It is especially problematic if best practice recommendations are given with disregard for research results at a higher or lower abstraction level. Additionally, theorizing between inputs, development, and outputs of ISP development seems to be restricted due to different abstraction levels (e.g., from the medium-level development process to low-level individual compliance). The abstraction levels presented here can be used to assess the position of a research contribution or recommendation and examine what lower or higher-level support is needed in addition to it in order to complete the ISP development process.

This dissertation aims to generate new research-based knowledge at the lower level of abstraction. It proposes ways to connect this knowledge with higher-level recommendations as well as other low-level knowledge. Having a deeper understanding of how IS rules are chosen can help in understanding the ISP development process at the medium level as well as the results of the development at the lower level. In other words, the significance of the lifecycle steps is revealed through the practices that take place within them.

3 THEORETICAL FOUNDATION

ISP development is essentially a combination of practices in which a series of decisions are made about the rules that employees should follow, with the aim of improving IS. This section introduces a theory that has been proposed to explain how people choose or create rules. Some ideas in the following subsection have been previously published in *Developing Organization-Specific Information Security Policies by using Critical Thinking* (Kinnunen & Siponen, 2018).

As the previous sections have highlighted, the ideal ISP reflects the IS needs of the organization in question. Whether the rules are strict and particular or general and open for interpretation (Siponen & Iivari, 2006), they still need to be thoughtfully selected by somebody. This selection process involves a moral component (Vance & Siponen, 2012). This dissertation uses Hare's (1982) normative theory from the field of philosophy to explain the thinking process behind making new rules. Hare's (1982) work was previously applied to IS by Karjalainen and Siponen (2011).

3.1 Creating new rules

Our thought process in how we follow and create rules has been the interest of moral philosophers for centuries. Hare (1982) presented a theory of moral thinking involving different levels, mainly intuitive, critical, and meta-ethical (Hare, 1982, p. 25). The idea of the levels is not new to moral philosophy but instead appears already in the works of Aristotle and Plato (Hare, 1982, p. 25). The theory is utilitarian, combining elements of the rule and act utilitarian principles on different levels (Hare, 1982, p. 43).

At an intuitive level, decisions are made according to the conventional rules we have learned (Hare, 1982, p. 45). This is the level of thinking we use much in our everyday life when we act according to the rules of society or our organization (Hare, 1982, p. 201). If only intuitive-level thinking is used when creating an ISP, the method might include listing components that we think are the right courses of action. This could involve copying rules from other ISPs. Such a method cannot resolve conflicts between rules or create new ones, even if the copied ones are poorly suited for the organization or conflict with other rules.

Critical thinking is used when rules conflict or when new rules are created (Hare, 1982, pp. 26, 40, 50). At the critical level, decisions are made based on careful consideration of the possible outcomes of the action. In the context of ISPs, it may be difficult to identify the issues that require critical thinking. Either there may not be enough knowledge about the situation to create rules, or there may be an expectation of general rules for the situation, and only intuitive level thinking is used. This may be the case when ISP developers choose controls from checklists (Baskerville, 1993) or even use a completely predefined ISP from a third party.

Critical thinking begins when we encounter a situation in which our existing rules do not apply or seem to be in conflict (see FIGURE 2). This requires an understanding of what relevant factors of the situation differ from previous ones. (Hare, 1982, pp. 52, 63, 89). Knowing who is affected by the rules and considering how they might feel about them are also important (Hare, 1982, pp. 92, 95). The answers to these questions are related to the scope, or the subjects and objects, of the policy (Baskerville & Siponen, 2002), and determining them requires gathering information about the organization.

Simply understanding the situation in an organization is not enough to make a decision about the rules that should be applied to it. The alternative choices for rules must be assessed in light of the relevant facts about the circumstances and the strengths of the preferences that the affected people might have (Hare, 1982, p. 124). When creating an ISP, this would mean that alternative rules should be considered from the point of view of the persons whose work they affect. This would include considering possible conflicts with other rules that affect their work. Taking the role of others has been suggested as an educational tool to teach moral judgment, which has a significant effect on ISP compliance (Vance & Siponen, 2012) and thus can help in making rules that can be complied with.

After considering the facts and outcomes of the different rules, it is possible to choose the principle to be used in the situation. This principle should be applicable to ISP subjects in a specific organization, but it cannot be expected to apply elsewhere (Hare, 1982, p. 200). Hare (1982, p. 212) does not present a universal algorithm for making moral decisions but rather leaves the labor of moral thinking to the people making the rules (Hare, 1982, p. 212). According to Hare (1982, p. 218), all that can be done is to make sense of the available facts and reason logically about the requirements of the decision.

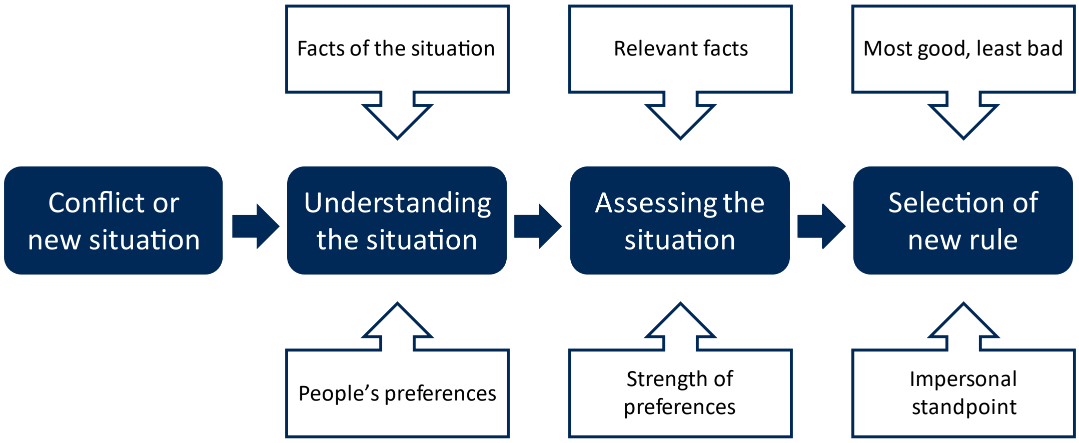


FIGURE 2 The flow of critical thinking

3.2 Critical thinking in information security rulemaking

Research has shown that if a person sees complying with an IS rule as morally desirable, they are more likely to comply (Myyry et al., 2009). This would indicate that it is prudent to include moral thinking in the rulemaking process to ensure a policy that is morally acceptable to its subjects. However, Hare’s (1982) method of critical thinking (1982) requires the ability to understand what the relevant facts are and how the alternative rules might be perceived by affected people. This kind of thinking relies on the highest stage of moral thinking, while Hare’s intuitive thinking represents a lower stage (Siponen & Vartiainen, 2004). This calls for a solution that guides rule-makers toward a higher level of moral development. When the rule makers are thought to understand the reasoning behind predefined IS rules, the role of information in their work, and how IS affects their work community, they may move toward critical thinking in the ISP-making process.

When a person is faced with the task of making an ISP, they may use both intuitive and critical thinking, depending on how they understand different aspects of the work ahead. When adopting general guidelines or recommendations into an organization-specific ISP, the person must be able to identify conflicts (e.g., with business operations) or new situations (e.g., background assumptions of the recommendation do not apply) to move into critical thinking. The research literature on ISP development suggests some themes and points in the development process when the adaptability of general guidelines must be evaluated against organization-specific situations. TABLE 3 lists examples of these critical points.

TABLE 3 Critical points of ISP development in the research literature

Theme	Literature mention
Requirements for ISP, Organization specific	"Generic and universal guidelines do not pay enough attention to organizational differences" (Siponen & Willison, 2009, p. 269) "The information security policy should never be written in isolation and will need to be supported by other relevant policies, standards, procedures and processes" (Höne & Eloff, 2002, p. 405). "We found a triangle of tensions related to the infrastructure affordances, economic realities, and social arrangements driving the process at MachineryCorp that originated neither from the InfoSec best practices guiding the development, nor from the organizational context, but from their interaction." (Niemimaa & Niemimaa, 2019, p. 18) "Over the years policies at various levels will have to be changed to accommodate new models of operation, new insights, and new organizational concerns" (Abrams & Bailey, 1995, p. 128).
Security and organizational goals /strategy	"Similar to other organizational policies, the security policy must maintain and complement the organization's business objectives" (Anton & Earp, 2000, p. 5). "Information security strategies employ principles and practices grounded in both the prevention and response paradigm" (Baskerville et al., 2014, p. 149). "The Perception Grid can help executives to review the alignment of information security strategy and the organization's overall strategy" (McFadzean et al., 2007, p. 654).
Connection to business model /processes	"A variety of reasons and explanations have been put forth for explaining the lack of effectiveness in the use of IS security policies, including that security controls often constitute a 'barrier to progress' and that security policies are very likely to be circumvented by employees in their effort to perform efficiently their tasks." (Karyda et al., 2005, p. 247) "We suggest that identification of value conflicts can be used as a strategic tool and opportunity to reflect on and improve health care practice" (Hedström et al., 2011, p. 382). "The lack of appropriate security controls on information exchanged among business activities in a business process can leave organizations vulnerable to information assurance threats" (D'Aubeterre et al., 2008, p. 529).

continues

TABLE 3 continues

Theme	Literature mention
User involvement; responsibilities and authority	"One of the difficulties for Information Security Managers is that often their role has been that of the technical specialist with a command and control approach to management. They have tended to take decisions concerning Information Security with little involvement or negotiation with employees.." (Ashenden, 2008, p. 198) "Perhaps the most critical role of the information security policy is to explicitly define the specific rights and responsibilities of individual users, and to communicate these successfully to each and every employee, so that a uniform, coherent and effective approach to information security is adopted across the organization". (Doherty et al., 2009, p. 450) "A rigid hierarchical structure may be a problem for information security management since the application of a security policy often requires organizational flexibility, including the creation of new roles or the adaptation of existing ones" (Karyda et al., 2005, p. 257).
Stance on guidelines / instructions / rules	"Both goal norms and principles leave the exact implementation to be decided, unlike rules, which prescribe in detail what to do" (Burgemeestre et al., 2013, p. 155). "Security policies and codes of conducts are frequently the main, or only, tool used by managers to guide and control employees' security behaviors" (Hedström et al., 2011, p. 373). "In the IS security context, establishing moral standards and preventing denial of personal responsibility play an important role in compliance attention" (Chen et al., 2012, p. 180).

This concludes the theory section of this dissertation. We started by studying the definitions given to ISPs in the research literature and found varying views on several aspects of the term. For this study, we selected a definition that broadly covers the IS goals and rules of an organization. From the definitions, we analyzed ISP development lifecycle models and inputs and outputs for the ISP development phase. The general development methods were complemented by aspects that the research found to contribute to organization-specific ISP development. These contextual aspects are key when we use the method of critical thinking to create new rules for an organization. We have identified some critical points in the literature that reflect the issues ISP developers should consider when creating new rules for their organizations. The following sections will move on to study these concepts in real-life ISP development projects.

4 RESEARCH APPROACH

We have discovered from analyzing the existing research on rulemaking in the ISP development process that it is a very complex issue with very few practical-level approaches previously applied to it. A qualitative research approach is required to understand the phenomenon better and more in-depth. AR was selected for this study because it allows for the deep qualitative analysis of the data as well as researcher involvement in suggesting new theory-based approaches.

4.1 Action research (AR)

The aim of this study is to find ways to improve the practices of organization-specific ISP development. The focus on practices situates this study at a lower level of abstraction in the field of ISP development research (see TABLE 2). Practices are the most tangible level of ISP development in which people sit around a table and have conversations about the policy content. Researching this kind of phenomenon requires a research method that produces rich and nuanced data on the situation. In addition to the data requirement, the research question calls for a method that allows the active participation of the researcher (Baskerville & Wood-Harper, 1998). In this way, it is possible to apply theory in practice and continuously improve how the solution works.

4.1.1 Action research as a method

AR was selected as the research method because it is well suited for situations where theory can be directly applied to practice, with the aim of evaluating and improving it (Baskerville, 1999). Any research method that could have only assessed the situation without resolving the problem would not have sufficed in this study from the point of view of the study subject or the goals of the research. The research problem requires a research method that is concerned with the real-life issues of ISP development and allows both researcher and practitioner input to solve the problem at hand (Baskerville, 1999; Iivari & Venable, 2009).

The research design adapted the canonical action research (CAR) principles (Davison et al., 2004) (see Appendix 3) as well as Baskerville's (1999) instructions. It must be noted that the CAR principles are not fully followed since they make assumptions, for example, about how much the researcher can participate in different activities during the research project. In this study, the researcher's active participation in some workshops would have created a conflict of interest. Due to this restriction, the "unfreezing" (Baskerville & Wood-Harper, 1998) is done when the ISP development process is changed and "frozen" again when the modified process is tested. In the action-taking (unfreezing) phase, the researcher acted as a facilitator for the change while the research subject made the decisions of how to exactly implement the suggested changes (Baskerville, 1999; Baskerville & Wood-Harper, 1998).

AR typically consists of cyclically repeated phases that are here called "diagnosing, action planning, action taking, evaluating, and specifying learning" (FIGURE 3) (Baskerville, 1999; Iivari & Venable, 2009). Data gathering in AR happens in social settings, where observation and interviews are used to understand the situation (Myers & Newman, 2007). In this study, the data collection methods were semi-structured interviews and workshops in the diagnosis and action-taking phases. In the evaluating phase, the solution was tested, and observation was done by remote connection (Skype, only sound) or in person. Notes were made from all meetings, and they were also audio-recorded and transcribed. The principles for evaluating interpretive research by Klein and Myers (1999) can be, to some extent, applied to this AR project. However, they created the principles for research settings in which the researcher is a passive observer rather than an active creator of the change.

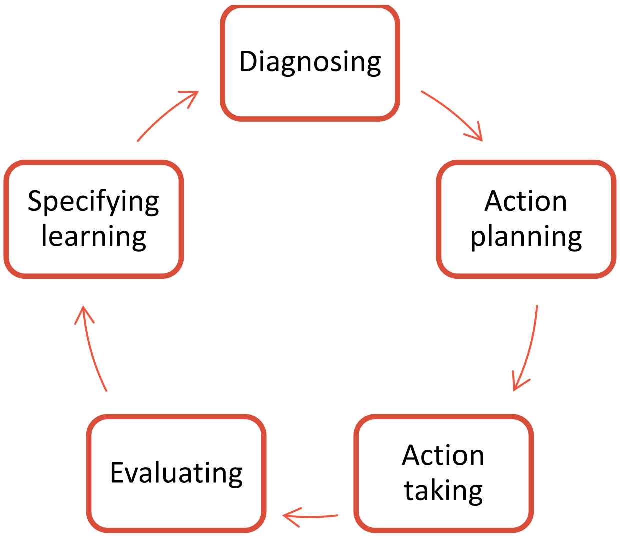


FIGURE 3 The action research cycle (adopted from Baskerville, 1999)

4.1.2 Theory building

The starting point for theory building in this study is Hare's (1982) theory of critical thinking, which explains people's thinking when they follow and create rules. The quality of a rule is reflected in how well it is able to reach the desired outcome. In other words, the point of the ISP is not to control people but to steer them into acting securely. To this end, it is vital that we understand what kind of thought processes are required from the ISP developers to create rules that serve their purpose. The theory explains how critical thinking is reflected in people's actions and thus gives us a way to analyze the way in which the rules are created. The concepts of the theory of critical thinking are used to explain people's actions and decisions in the ISP development process.

AR is not a research method that could, as such, reveal what people are thinking and thus provide evidence of the existence of critical thinking in the process. However, this method is at its best when analyzing and changing practices. Therefore, the theorizing is done using the practice lens that allows us to analyze what people are actually doing in organizations beyond the bespoke structures, such as the process model of an ISP development service. This view highlights human agency in this process and the repeated and improvised practices they perform (Feldman & Orlikowski, 2011).

4.2 Data collection

The aim of this research project is to improve the practices of ISP development. When an ISP is created internally in a company, the lifecycle usually takes a fairly long time, often at least a year, before ISP content creation is started again. For the purposes of iterative improvement, a shorter timespan helps in controlling the changes. A consulting company is an ideal subject for this research project since it can repeat the ISP development process several times in one year without losing momentum in making improvements. The changing customers also provide interesting data on the contextual application of general ideals.

The subject of the AR study is ISMcorp. It is a medium-sized (50-250 employees) Finnish company that provides IT and security management services to its customers. Its customer base was geographically spread around Finland and formed largely of SMEs. This research project focused on improving ISP development service. Before the project, ISMcorp had a service where it would create an ISP based on discussions with the customer and ISO27002. The service had been provided to a few customers before this project started. The application of the GDPR had recently spurred a marked demand for these kinds of services; thus, ISMcorp found it timely to improve their service.

The data collection period for this study was slightly over a year, from the fall of 2016 to the beginning of 2018 (see FIGURE 4). At the beginning of the research project, three other companies were involved in analyzing the problem and planning for solutions. The bulk of the ISMcorp data is from spring 2017. Due to the schedules of ISMcorp and its customers, the AR cycles' timeline had to follow the needs of the business. The overall study progressed unidirectionally through the phases of the timeline. However, there was some iteration in the steps when it was possible to go back to planning in the middle of taking action or assessing the action that had been taken and diagnosing the remaining problem at the same meeting (Davison et al., 2004).

All research data were collected by the author, but in addition to her, other researchers participated in some meetings. Data were collected in interviews and joint workshops with ISMcorp and the researchers. In the evaluating phases, the author also attended workshops as an observer. The meetings were audio-recorded, and notes were taken. Later, the recordings were transcribed and coded to keep track of emerging themes in nearly 400 pages of data.

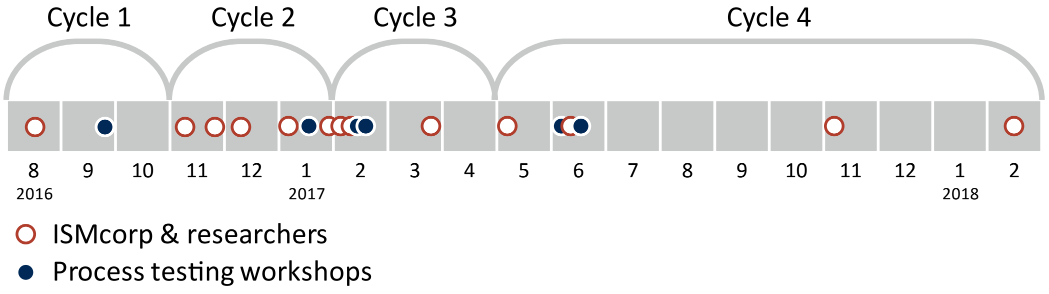


FIGURE 4 Research timeline

4.3 Researcher–client–agreement

Davison et al. (2004) provided a list of criteria for a successful researcher–client–agreement in AR, which are here used to explain how the relationship was formed with the research subject. The agreement was formed in two stages. First, formally, when the university researchers and ISMcorp applied for funding together and agreed on the topic and general scope of the project. Then, when the project actually started and the details were negotiated.

ISMcorp wanted hands-on help and recommendations from prior research to develop its ISP development service. It was agreed that AR, with joint action, would be the appropriate approach. The service that was the focus of this study was already clearly defined, and the goals for its improvement were discussed. It was clear to both parties that much of the project schedule would be influenced by ISMcorp's customers. Both the university and ISMcorp had already committed to producing the results when applying for funding for the project.

During the first steps of the research, four key persons were involved: a senior and junior researcher (author) (from the university), a chief development officer (CDO), and an IS officer (from ISMcorp). The senior researcher and the CDO were mostly involved in the first cycles, while the junior researcher and the IS officer were in charge of data gathering and taking action until the end of the project. ISMcorp was also very open to researchers observing the service in practice and secured permission from their two clients for the junior researcher to observe their ISP development.

Identifying the actors in this research setting is also important from the point of view of understanding the practices they enact (Niemimaa, 2016). ISMcorp and customer company representatives are the actors who enact the practices related to the ISP development process. ISMcorp people's actions are influenced by recurring practices developed in the company with other customers and knowledge of IS "best practices." Customer people's actions are influenced by their organizational and business field-specific practices.

5 RESULTS OF THE ACTION RESEARCH STUDY

This section discusses the four cycles executed in the AR project, where the aim was to improve the ISP development process with ISMcorp. The first cycle stands out as different since it laid the groundwork for the rest of the study. After the descriptions of the cycles, the results are discussed through the theory that emerged throughout the study. Since IS is a delicate issue for the participating organizations, many precise details are not included. The preliminary results of this study were published by Kinnunen and Siponen (2018).

5.1 Cycle 1: Theory refining

The first cycle in this AR study was significantly different from the rest of the cycles. The goal of this first cycle was to build the foundations for the interventions in the later cycles. The data in this cycle was collected from four organizations.

Diagnosing

The AR project started with interviews with four companies, one of which was ISMcorp. The interviews were semi-structured and covered the same themes that were identified as critical points of ISP development in the research literature (see TABLE 3). The inclusion of several companies in this first cycle allowed for a more general understanding of the issues that companies face when creating an ISP. The goal of the interview was also to gain knowledge about the specific problems ISMcorp felt they had with their ISP development.

The participating companies were:

1) a small consulting company providing IS services to customers, mostly in highly regulated fields;
2) a large corporation in consulting and ICT services with customers in public and private sectors;

3) a medium-sized company providing ICT design-related services in a highly internationalized value chain.
4) ISMcorp

ISMcorp and company 1 provided ISP development as a service for their customers, while companies 2 and 3 were interested in improving their internal ISP process. In each company, the interview was done with a contact person who had a responsibility to improve the ISP process. At ISMcorp, the first interview was done with the CDO.

Action planning

The first intervention in this AR study was planned as a workshop. In preparation for the workshop, five themes were derived from the research literature (see TABLE 3) and the interviews in the diagnosing phase (see TABLE 4). The researcher also prepared a presentation explaining the ideas behind these themes. This first intervention was designed to stimulate the participants into thinking about ISP development in new ways. There was no expectation that the first intervention would significantly improve the ISP development process but instead yield a better understanding of the issues for the next diagnosis phase.

TABLE 4 Themes in company interviews

Theme	**Interview mention**
Requirements for ISP/ Functions of ISP	'Must be measurable to make sure goals are achieved' 'Following the ISO27000 standards, the ISP must reflect commitment to continuous improvement' 'ISP is there to make people aware, not usually detailed checklists on what to do' 'Policy is a rulebook of what is done on the organization level' 'ISO27000 works as a basis and requirements come from the organization and environment' 'Requirements may come from government instructions for secure operations' (Finnish Katakri) 'Changes in the regulation or customer demands may be a cause to update the ISP'
Security goals/ strategy	'ISP describes the spirit or aim and is connected with business strategy' 'Policy must define practices for inspections' 'The ISP should state security goals; they must be reachable for that organization and reflect the level of risk the organization is willing to accept'

continues

TABLE 4 continues

Theme	Interview mention
Alignment with business model/ process	'Connected with customer requirements' 'The global business might cause issues, we need a unified arrangement' 'ISP and risk management should be planned with the processes built-in' 'It is significantly easier to get a person to follow the ISP in their own work if they were involved in creating the rules instead of just giving them a piece of paper containing rules' 'If a company wants real information security, then they must think about the real ways of working and from that infer the general guidelines' 'It is good to use the same practices that are used to monitor other activities' 'We should be able to push the idea to all business units that security must be a part of all business activities.'
User involvement	'Is a mandate from the top management and not written by the IT manager' 'The different unit leaders should be responsible for developing the parts of the ISP that concerns them' 'There is a general level that should be applicable to anyone but then there is the project/program level where people should check it if there are special requirements' 'For example, if the theme would be personnel safety, then we would pick connected themes from the standard, the HR representatives would bring the business view and we would whine about information security' 'If people start to go around security rules, it's because the business people weren't involved in making the ISP' 'It's not a thing for the lone hero but the entire organization' 'Often there is a core group and interviews with business areas' 'In one case, we asked the employees who use social media to make the policy for social media use instead of the manager who didn't know anything about it'
Guidelines/ instructions/ rules	'The lower level documents under ISP include must, may, and should types of guidelines' 'The whole policy is not meant for everyone; instead, it consists of different parts like the instructions for mobile work, and the ISP rules are included in other personnel guidance like recruiting guidelines' 'The ISP should not have particular working instructions that change often but instead be a basic support for practice'

Action taking

The workshop participants came from ISMcorp (CDO), the researchers' university, another university, and the previously interviewed people from the three other companies. The idea was to share thoughts about ISP development, which was facilitated by introducing the five themes one by one to the participants and then asking them to write down thoughts about them on post-its. For each theme, the participants were asked to think of principles and practical ways of executing them in the ISP development process.

The first theme was the requirements of the ISP and its functions. Many post-its mentioned requirements that come from within the company, such as the business processes, goals, and previous ISPs, and the way to get information about them is through users and experts in the organization. Risk assessment and customer demands could also be business-driven requirements. The use of standards and best-practice documents was also mentioned as a source of requirements.

The next theme was security goals and strategy. Many mentioned that they should be linked to business strategy and support it. Goals also sparked ideas about measuring how they were reached. Some suggested that a high-level strategy would be the first thing to state in the ISP development process and should be the first thing in the policy to justify the content and create buy-in.

The third theme was the alignment of business processes and models. Understanding the business processes and business model helps in determining what information is vital to the organization and where the focus of IS measures should be. Many expected that there would be conflicts between IS and business operations. To remedy this, continuous alignment efforts and dialogue with staff were proposed.

The fourth theme was user involvement. Two groups were mentioned in many post-its: top management and end users. One note said, "Policy creation should be guided by management and informed by users." The main reason for including a wide range of people from different parts of the organization horizontally and vertically was to create buy-in and awareness in the ISP creation phase.

The last theme was titled "guidelines/instructions/rules," and the participants were asked to think about both the nature of the statements in an ISP and their internal hierarchy. Some mentioned a multilevel architecture that should address both high-level and operational-level concerns but should not be too specific about naming people and systems to avoid constant revisions. Adaptation to changes in the operational environment or business strategy was, on the other hand, mentioned to be a good reason to check if revisions are needed. Constant monitoring of compliance and building a security culture were also mentioned as things that could be affected by the way an ISP is formulated. This would suggest that rules in managerial policies could be overridable, and this is why it was suggested that exact compliance with exact rules should be facilitated by technology.

Evaluating and specifying learning

The workshop allowed the participants to share their ideas about ISP development and to hear how people in other organizations view the matter. This was the first attempt to stir new kinds of thinking about ISP development among the participants. However, the five categories were too abstract to yield many descriptions of how these themes might be acted out in a practical situation. Most comments on these categories were abstract ideals rather than pondering how the themes could actually be included in the ISP creation work.

Despite this, there were good ideas on the post-its, and they provided material for improving the intervention for the next cycle.

5.2 Cycle 2: First internal test – we had no idea

This second cycle was the first one where only ISMcorp and the researchers were involved. The theoretical intervention was further developed and used in the intervention where the ISP development process was improved.

Diagnosing

At the beginning of the second cycle, the first step was to diagnose the problem in order to move toward action planning. From this second cycle onwards, the focus of this study was only ISMcorp. In the previous workshop, it became apparent that the five presented themes were too high level to induce many ideas about how the ISP development process should be done in practice.

During the diagnosis phase, the CDO from ISMcorp gave a presentation about their ISP development and implementation service at an event. The presentation highlighted some of the issues about ISP development that had been discussed in the joint workshop in the previous cycle. He started by explaining how some see the ISP only as a high-level declaration with no practical use or a useless document that has no benefit to IS. ISMcorp, on the other hand, based its IS services on the notion that ISP is a playbook for achieving security coals with different levels and means for practical work, as well as continuous monitoring and improvement. He then moved on to talk about how some develop ISPs by copy-pasting Google search results or by the hard work of a single individual. His solution to prospective customers in the audience was to order the ISP development service from ISMcorp. Their service promise was to create a policy based on business needs, acknowledge risks, be realistic, engage with the company, and provide ready-made structures and contents. Lastly, he spoke about the implementation of the policy, which is often done only by sending a mass email or training a few people, hoping they will teach the rest. The ISMcorp solution was to create the foundation for implementation already in the ISP development phase and then continue with monitoring, communicating progress, engagement, and continuous development. Based on the first interview, we knew that this service promise was the desired state and not the current situation of the ISP development service. These service promises were used as starting points for further improving the ISMcorp ISP development process.

The second cycle diagnosis was continued in a workshop with the researchers and several ISMcorp representatives. The CDO explained that he wanted to do ISP development in a way that is business-driven and makes people in the customer company really committed to it. The need was to have a process that was repeatable across different kinds of customers but also be driven by the customer and their feedback. He hoped to get some ideas to improve the plans they had then and wanted to do an internal test of the process. Their goal was to obtain IS certification for ISMcorp.

The current situation of the ISP development process was that it had adapted modules from the ISO27002 standard (Finnish Standards Association, 2014) and adopted them into a content management system (CMS) that would be used for documentation. Then, each module would be discussed with the customer in a workshop where the participants would be from the business areas that the module concerns. After the policy workshops, the entire policy documentation can be finalized in the CMS system. Lastly, they would do a security strategy document for the executive management that would basically be a summary of the most important parts of the ISP. The strategy was created last because an understanding of the customer's business was formed in the policy workshops.

When asked about what should be further developed in the process, the CDO first said that it should be less time-consuming both for them and their customers. They also wanted better ways of getting customer feedback during the process. Implementation was also seen as a challenge that could be tackled in the ISP development phase. One such thing is stating responsibilities so that the regular policy reviews would have a good representation of the key persons and management involved.

The researchers and ISMcorp representatives talked about how things could be further developed. A researcher suggested that relying too much on a standard in the development process could turn the development process too much into a checklist kind of action. That might lead to losing focus on what is essential for the customer and how the policy can be implemented. The CDO agreed and said that there was much redundancy in the standard, especially for an SME, and they hoped that the policy structure could be checked within this project.

Action planning

In the diagnosing workshop, the researchers suggested looking into critical points in the development that could help get the customer involved in creating an organization-specific ISP. For example, different customers may have very different needs for the confidentiality, integrity, and availability (CIA) of different information depending on their business model. The customer could be asked how critical these things are. The idea would not be to add extra content to the ISP since the ISO27002 framework is extensive enough but to go deeper into the areas that are important to the customer.

The discussion then moved on to creating ideas of what these critical points could be. Measurement was mentioned first regarding whether it is prudent to measure policy compliance or whether IS is actually improving. Then, the discussion moved into long, hard-to-read policy documentation, which the CDO exclaimed: "should be banned." This stirred conversation about signing papers for liability and taking checkbox tests for IS because these things are measurable and easy to explain to executive management. Instead of being concerned about how many have passed the test, executives should be interested in the value of the organization's information and how much could be lost if security measures are not truly effective. It was clear that there would be no simple solution to address this.

The first cycle and the diagnosing workshop with ISMcorp helped the researchers analyze the situation further. The five themes discussed with a larger group in the first cycle yielded more information about the things that these companies deemed problematic or important in ISP development. These ideas, together with reformatted themes identified in the literature (see Appendix 2), were now formed into 11 critical considerations (CCs). Their purpose was to steer the ISP developers toward understanding and assessing the situation where the new ISP rules would be applied in. These CC would be used in the later action-taking phases as catalysts to improve the practices of ISP development.

Action taking

The CCs were presented to the ISMcorp representatives (including the CDO and a new IS manager) in a joint workshop. Each CC was supplemented with ideas about how the CC could be included in ISP development. The goal of the researchers was to help ISMcorp see its development process in a new light. It was especially emphasized that the CCs didn't represent steps in the ISP development method, and they could be applied to the process in different ways. The CDO and IS manager commented on the CCs, giving more insight to their views about ISP development (see TABLE 5).

During the workshop, the CDO became convinced that moving forward with identifying risks, processes, and technology before ISP creation would be the right way to do it. At the beginning of the ISP development project, there would be a workshop where they would first draw a process map with the customer to visualize the operations of the company, and then they would collect more detailed information about the processes, such as criticality, key person, owner, and digitalization level. This is how ISMcorp could show customers that they are doing business-driven ISP development.

ISMcorp had its CMS system at the heart of the ISP development process. It was used to gather information about the customer for further use in ISP development. It was discussed that the system could be modified to better support the gathering of information about customers.

The framework for the policy development workshops was adapted from ISO27002. The CDO felt that there was too much repetition of the same things from different angles, and it would be difficult to keep the customer engaged in the process if the excess was not trimmed out. SMEs, in particular, are not interested in a large-scale ISP development process, but they want consultants to take care of IS (especially personal data protection because of legislation). To this end, the CDO wondered if they could just do a heavy copy-paste of a general ISP that they created for SMEs. Then, they would start to modify it to organization-specific requirements in yearly reviews.

TABLE 5 Comments on CCs

Critical consideration and short name	**ISMcorp comments**
The organization's management is motivated to take action toward information security *CC management motivation*	Understanding how risks could affect business continuity and profit. News coverage on ransomware has made managers realize that cyber threats can holt the entire business to a standstill. Often information security is seen as an IT issue, but it is possible to help the managers see that it affects everything. Especially in SMEs the managers often have the notion that no-one would be interested in them.
ISP is aligned with business strategy *CC strategy alignment*	The strategic level development starts with trying to understand what is really important for the customer business. The strategic level decisions (such as is information security allowed to make operations more rigid) have to be agreed with the managers first before it is possible to fine tune the operational level rules. Often SMEs don't even have a documented business strategy. The information security strategy should acknowledge that perfect security doesn't happen overnight, but the strategy must define the steps that must be taken to reach it.
ISP is defined in a way that is comprehensible to the organization members/subjects *CC: Comprehensible documentation*	Some see that a policy should be one A4 paper with a line for a signature at the bottom. That is not a policy, it's a way of implementing a part of it. The policy must cover everything important. On the operational level the policy documentation is not meant for everyone to read but it is built into the work instructions. This can be a real problem if a person is trying to find out how they are supposed to act in certain situation and the policy documentation doesn't seem to give answers. Must have dialogue between the consultants and the customers. The language will automatically be intelligible if ISP creation is based on business needs.
Understand the operational context of the ISP *CC: operational context*	Laws and labor unions can have a big influence on the scope of the ISP. Then again business must go first and if for example a standard says something, but the company would benefit more from going against it then I would advise doing what's good for business.
Stakeholder groups/people affected by the ISP are identified *CC stakeholders identified*	Hard to comprehend what this means. If ISP is created with ISO standard, then different groups will be covered. Maybe this could be a part of the motivation in the beginning of ISP project and improved customer relationships could be used as motivation. This could be interesting for internationally operating companies.

continues

TABLE 5 continues

Critical consideration and short name	**ISMcorp comments**
Security requirements are determined at the company level *CC organization requirements*	Companies in different fields have very different needs (e.g. CIA in different systems). This connects to processes. If we know the critical processes of the company then we start to understand what is important to them. This needs to be in the beginning of the process. If we identify processes, then we know the business and key persons. Process maps allow people to conceptualize their own work.
ISP specifies the information affected by the policy *CC defines information*	This is not very different from the previous one. If the information criticality of the process is defined, then this is done too.
Authority and responsibilities are stated *CC authority & responsibility*	Technology, processes, and policies can all have owners and key persons. When a person leaves their position it should be easy to find out from the CMS system what their responsibilities have been. There must be a balance between the responsibilities of people and how much their actions are limited with technology.
Indicators for compliance and goals are built into the ISP *CC indicators for goals*	Policy should not define metrics but be built in a way that it is possible to observe if the ISP has been implemented well. There are things that can be easily measured technically and others that require asking people with, for example, surveys.
Information security development and maintenance are connected with the business processes *CC connected with processes*	Mapping processes will be an easy way to learn about the customer's business. This is what we will do.
Policy is evaluated and tested in the organization *CC evaluating and testing*	This has been done before only by seeking approval for the finished ISP document from the top-management. This should be done efficiently. Maybe having people on board in the ISP development and asking their comments about the fit of the rules to the real daily work.

These discussions lead ISMcorp to do some changes in their ISP development process and the corresponding parts of their CMS system. At the end of the action-taking phase, the process had four main parts: project introduction, process workshops, policy workshops, and review (see FIGURE 5). The project introduction now included management motivation and planning for the participants in the upcoming workshops. The process workshops would include mapping higher-level processes, evaluating their importance for the business, describing the processes and their key persons, and finally, giving CIA values for the information used in the process. The results of the process workshops would yield a risk report, which would then be used as the starting point for discussing the content of the ISP. The policy workshops still followed the structure of the ISO27002 standard. After the workshops, the consultant would take all the information he had gathered and write it up as a policy. Lastly, this document would be reviewed by the customer.

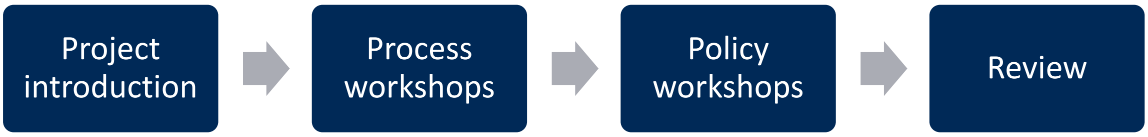


FIGURE 5 The planned ISP development process

Evaluating

The changed ISP development service was evaluated by testing the process. The first run of the new ISP development method was done as an internal test at ISMcorp. The aim was particularly to practice the new process workshop of the ISP development process. The workshop had four participants: the CDO, the IS manager, and two other high-level managers at ISMcorp. During the internal test, they focused only on the beginning of the process workshop, where the company's processes were mapped out and their importance was evaluated. The IS manager explained the process to the other participants, but the other parts of the workshop were led by the CDO.

ISMcorp had already mapped some of its processes earlier for other purposes. The CDO had begun to make the process map before the workshop, and there were other processes already described in the CMS. This meant that the discussion was mainly about updating the information and checking that nothing was missing. The exercise prompted a lively conversation about the current situation and the future plans of the company, especially because the workshop participants had such a high status in the organization.

The CDO noted that the participants' different views of the processes and their hierarchy helped in sharing an understanding of the realities of business operations and how they conceptualize individual tasks into larger entities. One of the other participants wished they could have also addressed how the processes were linked together to gain a more comprehensive view of the situation. They also noted that some of the processes were tightly linked to their customers and that customers' processes played a big role in how certain processes were executed at ISMcorp.

The group had time to map out and evaluate the importance of only two areas of their business operations. The CDO said that they would conduct the next step, which was descriptions and CIA evaluations, only for critical processes; therefore, the evaluation was important. The group valued a large portion of the processes as critical and even wanted to give entire process groups the same critical value. The importance evaluations of the processes would later be used to monitor the processes and how they change over time. Because of the changes in evaluation and the new scope and hierarchy of many processes, the old process descriptions would need to be checked and updated next.

After the workshop, the CDO thought that they had done much less in the time they had than he would have expected. He still believed that the process mapping would be faster with the clients since they did not have any maps ready, and that would mean that they would not go into as much detail. He also considered the possibility of first starting with only business areas and process groups in the workshop and then allowing the customer to do most of the process mapping and evaluation independently. They had also originally planned to include IT-related issues in the process descriptions, but these were deleted since they would have been too laborious to map out and would have led the focus away from managerial ISP creation.

In an interview, the IS manager explained that the process mapping and descriptions took four meetings in total and went far deeper into detail than the security scope would have required. The participating managers also started to make plans to improve the processes during the workshops, even though the purpose of the workshops was to build an overall picture of the current situation. The IS manager thought that the process map should be updated far more often to avoid discrepancies evolving in managers' views on how processes link together.

Overall, the IS manager felt that including the researchers in developing the service had opened his eyes to thinking about the ISP development process on a more theoretical level. He thought that, in particular, the start of the process had improved. It helped in weaving the organization's operations and IS together, unlike the old method, which easily led to the dual development of security and business practices.

Specifying learning

This was the first cycle where the CCs were used to stir ideas about the ISP development process. The ISMcorp representatives seemed to understand the importance of most of the CCs in the action-taking phase, but it did not lead to changes in the process. The internal test showed that while, for example, the management motivation had been added to the process chart, it did not really translate into practice. The CC on aligning ISP with processes received much attention, but the negative effect of adding work to the process seemed to be more important to ISMcorp than the possible benefits. When considering the changes from the critical thinking perspective, it would seem that mapping the processes contributed to understanding the situation better. The complexity of the policy subjects and objects became more pronounced when the participants tried to visualize the whole situation.

5.3 Cycle 3: First customer – time optimism

In this cycle, the most significant revisions to the ISP development process were completed. The process was tested with a real customer organization for the first time.

Diagnosing

After the first two cycles, the ISP development service changed quite dramatically. First, the changes had been at a higher level, and the CCs had been included more as guiding ideals. However, there was still much to do with creating useful practices that could be repeated across customers.

From the internal test, the it was learned that keeping the discussion in the process workshops at the correct abstraction level was difficult. In the internal test, the workshop participants were operational management, and it would be the same case here. Therefore, the IS manager expected that it would be hard to stop the customers from going into too much detail and planning. That, again, would lead to the need for more than one two-hour workshop on process mapping.

Action planning

There were no new theoretical constructs added in the action-planning phase of the third cycle. Only a few of the 11 CC were thus far used to inform the ISP development process. The plan was to continue suggesting new practices based on them. The previous cycle had proven that the process workshops could be time-consuming. However, they played a vital part in helping the organization members understand the situation. To this end, the recommendations planned for this cycle were to improve the workshops.

Action taking

When the AR project reached the third action-taking cycle, the practices and systems included in the ISP development process were modified further, but large changes were not needed. The IS manager was fairly confident that the process was ready to be tested with a real customer. However, as the first workshops with a real customer drew closer, he was concerned about facilitating the workshops in practice. The CMS system that was needed to gather information was still under construction by the CDO, and new security-related features were added. This meant that the IS manager had little time to learn the new features and how to operate the system to use it while facilitating the workshop. This could be an issue since the information collected in the customer workshops is used in the later phases through reports, and there was confusion about what the reports would include.

The CDO had a major role in planning the process and CMS system, while the IS manager was the one who would take it into action with the customer. Features like process owners and evaluation tools were further developed after discussions about CC *authority and responsibility* and CC *organization requirements.* Just before the first process workshop, the CDO trained the IS manager to use the new features he had created in the CMS system. His view was that the process workshops would train the participants to think from a security perspective and, on the other hand, help the IS manager identify and comprehend operational risks. In the previous version of the ISP development process, the risks were identified using general templates, but in the new version, the risks could be derived from the information gathered in the process workshops.

Changes were also made for the later parts of the ISP development process. In the policy workshops, the IS manager would go through the ISO27002 standard contents in the themed workshops by using clarifying discussion points. After the policy workshops with the customer, the IS manager would finalize the policy document.

The CC *indicators for goals* inspired the CDO to add a selection of predefined controls to the ISP process. He tasked the IS manager to think of controls that could be monitored. The idea was that the IS manager would select and suggest to the customer some implementation tools and metrics that would fit their new ISP and could be added to the yearly follow-up plan. This addition was made because, before, in the yearly reviews, customers would have provided their own views on how things have progressed, but there had been very few ISP-specific metrics to discuss. The IS manager designed a new list of controls that could be easily monitored with ISMcorp's tools. The customer could be given choices of the controls they wanted.

The CC *connected with processes* still had the most prominent role in changing the ISP development process. After the experiences in Cycle 2 and previous customer relationship with the first organization, more changes were made to the process workshops. The process workshop working order was changed so that the process descriptions could be done immediately after the mapping. This change was done to help the participants gain a security mindset that would be needed in the policy workshops.

Evaluating

The first real customer (Customer 1) for the ISP development service was a medium-sized (consolidated) company operating in the manufacturing industry. They had been a customer of ISMcorp services before in IT management services. Customer 1 approved that a researcher could observe their workshops and that the ISP development service offered to them was a new and improved one. The initial timeline for the project was that the process and policy workshops would be done within two months, then there would be a break of around six months due to their production schedule, and the policy approval and implementation planning would come after that.

The ISP development project at Customer 1 started with a start-up meeting with the IS manager and Customer 1 IS officer, executive board members, and business area managers. The original plan was that this meeting would include a discussion of the project progression, the kind of ISP that would be created, recruitment of people for the workshops, a discussion of the business strategy, and an analysis of how IS goals could be linked to it. However, the plans for including strategy discussions in this part of the process were not finalized and were missing from the agenda of the meeting.

The process workshops at Customer 1 started similarly as in the previous cycle since they had some processes already mapped. These, however, were mapped from the IT governance side and not really from a business point of view. This has led to the importance of evaluation being done more from an availability standpoint and not evaluating its value to business operations. The evaluations were not straightforward and seemed difficult for the participants. The IS manager even told the participants to make a criticality evaluation from an IS point of view instead of considering business criticality. When the discussion moved away from the previously mapped processes, the IS manager was better able to steer the discussion toward the business criticality of the processes.

The process workshops helped the customers better perceive the information used in their processes and their security needs. For example, a customer had trouble understanding how the CIA evaluations could be applied to their invoice process. The IS manager presented a hypothetical situation in which the invoice was accidentally sent to the wrong recipient. This made the customer understand that the invoices contained information about other customers, as well as product prices, which were not public information but a result of negotiation.

After the process workshop, Customer 1 moved on to the policy workshops, which covered 14 content areas from the ISO27002 standard. Before this process, Customer 1 had only a partially stated ISP in their ICT manual, but not a full IS governance structure and policy. The reason they wanted to create a comprehensive ISP was that their company had grown larger, and new regulations, such as the GDPR, had changed the requirements for IS. In addition, their partners were asked to view their policies in e.g., contingency planning.

The fact that the policy workshops had been planned based on the ISO standard caused some problems in redundancy and the order of the topics. For example, the workshops started with agreeing on some more general principles of the ISP, but that included determining the confidentiality level of the policy documents. The customers were unable to give a useful answer since they did not know what the policy would contain.

Another reason why the customers could not give useful answers to questions was that not all of them understood their role in the process and what was meant by many of the policy topics. For example, the IS manager asked if Customer 1 had any procedures in place for partnership management. Person A suggested that Person B managed most of the supplier relationships. Person B said that he was only in charge of procurement but knew nothing about IT—that was the responsibility of Person C. This shows that not only did Person B not understand how IS is connected to all parts of the business operations (not just IT), but he also did not understand that he was invited to the workshop to share his expertise.

A frequently recurring theme in the discussions was that the customer expected the IS manager to tell them how things should be done “right.” For example, the IS manager asked whether their IS policies should be reviewed and who should do so. The customers disliked the idea of laborious inspections and asked if they really needed to invite an external auditor to do them right. It did not occur to them that they could decide on anything, from an internal random check every five years to full yearly audits performed by professionals. The ISO27002 text suggests that the review could be done by an "internal audit function, an independent manager, or external party organization specializing in such reviews" (Finnish Standards Association, 2014). This is a good example of a situation in which the IS manager (or the standard) would have benefited from having prepared a range of alternatives and explanations for their convenience-risk trade-off.

When evaluating the process and policy workshops with the researcher, the IS manager thought that the discussion had gone too detailed. Similarly, as in the internal test, the workshop participants began to scrutinize dysfunctional processes and make plans for improvement. While these discussions are important for improving operations, they do not add any extra value to the ISP development process.

The IS officer from Customer 1 commented positively on the ISP development process after the workshops had been completed. He thought that the process was interesting and that people in their organization had learned a lot. However, some workshop participants did not get as much out of the experience and seemed like they would much rather be somewhere else.

While the workshops had generally been a positive experience for the participants, there were many things that could still be improved. As the process was changed just before the workshops, the IS manager had to put extra effort into running it formally, as planned.

Specifying learning

Many of the CCs that had been discussed with ISMcorp were not fully embraced in the practices with Customer 1. Some ideas had been included in the process through changes to the CMS and workshop slide sets. However, many of the positive effects that were envisioned did not translate into workshop practices. This cycle highlighted how sensitive to the customers' signals the IS manager needed to be in the workshop situation to be able to, for example, collect business-level requirements or make sure that everyone comprehends the terms that are used. This shows how difficult critical thinking can be as a group effort. Each workshop participant knew different facts about the situation and had different feelings about the alternative rules but communicating them required skillful facilitation from the IS manager.

5.4 Cycle 4: Second customer – what does it mean?

In the fourth cycle, the ISP development process was not dramatically changed anymore. The improvements happened in the finetuning of the workshop practices. The process was tested for the second time with another customer. This was the last cycle, after which the project was ended.

Diagnosing

Based on the lessons learned from the previous cycle, the IS manager thought that the way in which the strategy and processes were covered in an ISP should be improved. In his view, there was a need to get people in the right mindset for the entire time period when the workshops were held (a few weeks ideally). He felt that people had not thought about IS at all before and had just come into the workshops to listen. People at Customer 1 were very easygoing and jumped right into action when asked.

On the other hand, the CDO and IS manager had come to the conclusion that the time that was spent in the process workshops with Customer 1 had been too long. The idea was to only make them aware of the connection between IS and local processes. The conversation had taken too long and ended up more than double the time that was reserved for it.

Planning

The issue of time management in the workshops was an indicator that the IS manager needed help creating practices for facilitating the conversation.

Alignment to the business strategy was added to the beginning of the process description in Cycle 2. However, this step was not completed in the previous cycles. The CC *strategy alignment* was chosen to propose as one remedy to guide the conversation to a suitable level for ISP development. It could be connected with CC *management motivation* since the strategy phase of the process was aimed to the customer's top management.

Action taking

In this cycle, it was clear that the issues with the ISP process resided in the workshop practices. To resolve these issues, the researcher and IS manager had discussions to finetune the service. The conversation moved from the ideas behind the CCs to practical facilitating techniques.

The IS manager was afraid that people at the next customer (Customer 2) would be more reserved and that he would have to force the answers out of them. He thought it was problematic that he could not share the workshop materials with the customers beforehand since they were ISMcorp intellectual property. Then again, adding training sessions for the workshop participants would be overkill since that would add more meetings to an already packed schedule.

With Customer 1, the workshops had been too long, and the discussion did not stay at the appropriate abstraction level. To remedy this, the IS manager planned to turn some of the finer details of the process workshops into "homework." The plan was to map the high-level processes together and guide the customers to evaluate criticality and write down process details without help from the consultant. The researcher suggested that the customers could choose to have their own workshops or do the work individually for different results. The drawback of this plan was that without the consultant present, there was the danger of the customer losing focus and not doing the groundwork needed before the policy workshops.

With Customer 2, the process workshops were divided into business areas. This meant that a single person would not have to stay focused on the task for more than two hours when their own work was being described. One issue that might drag out the workshops was the fact that Customer 2 had invited many more participants than Customer 1. This could potentially affect the participants' motivation. The IS manager was afraid that there would be only a couple of people speaking and another 30 "yes-men" quietly sitting there. He thought that one way of fixing the issue might be to simplify the matter even further, but he was worried that the point might be lost. He also planned to have the participants prepare more for the process workshops so that they would better serve as just a communication tool between the consultant and the customer regarding how the company is operated, and any discussions on improving the processes would be done internally.

Evaluating

In the fourth cycle, the ISP development process was tested with Customer 2. It is a medium-sized (consolidated) company in the field of critical infrastructure. This company had already been ISMcorp's customer in different services. For this ISP development project, they came in with schedule issues related to their businesses' yearly cycles.

The process at Customer 2 began with a "re-start" meeting, as they had already started the ISP development process earlier with ISMcorp using the old service process but never finished. They had decided to restart the process with more effort, especially since the new GDPR made it a topical issue.

At this starting meeting, the company executives explained their commitment to the process. They were also asked questions about the company's strategy. The ISP development process was introduced to prepare the participating managers for their business unit process workshops. At this point, a person from the marketing team protested mapping processes since they were already doing the same thing internally for their unit and did not want to spend time doing it all over again. The IS manager had to explain that any existing process descriptions would make the workshops easier. It was lucky that the customer brought this issue forward since collecting and using existing documentation were problematic in the two previous cycles as well but never resolved.

The processes were mapped in business unit workshops. While this ensured that everyone was closely connected to the processes they were mapping, problems arose from processes extending across the two units. The participants had lengthy discussions about invoicing, where one unit would take care of it from a bookkeeping perspective while another unit would make sure that the billing information was correct. This was a situation in which it would have been beneficial to have a cross-unit workshop. One workshop participant exclaimed that it was dangerous to leave gray zones in undefined processes that span business units since that could lead to a situation in which no one takes responsibility for a process that might be in bad shape. The IS manager explained that it is possible that the processes are not described perfectly, but this is why every process has its owner and key persons so that there would be named people who should monitor their process and related processes for possible issues.

From the previous cycle, the IS manager learned how to guide the workshop participants through challenges in evaluating the importance of processes. Again, the customers wanted to mark almost everything as business-critical. The IS manager asked if these processes were really the ones that created profit. He explained that critical processes meant the ones needed to run the business. Something that might increase profits in the future, such as development projects, might not be critical from an IS perspective. He reminded the participants that this evaluation was done so that in the ISP implementation phase, they could first prioritize fixing the processes that are vital to business continuity and in bad shape.

While the IS manager improved the guidance in the importance evaluation, there could have been similar developments in explaining what the CIA values mean. The customers had real difficulties in trying to understand, for example, the availability of their processes. One process workshop decided to take time out from the process descriptions to write down the definitions of confidentiality, integrity, and availability on a whiteboard. This exercise actually helped the participants grasp the meaning of these concepts, and after a slow start, they were able to finish the descriptions in the reserved time.

In this cycle, the IS manager gave the customers homework to keep the workshops short enough. The process map was finished in the workshop, and the process descriptions were started; however, if there was no time to finish describing every mapped process, the group would continue later on their own. At the end of the workshop, the IS manager gave the participants an Excel template and asked them to write down the rest of the descriptions later, which the participants happily accepted.

Compared to Customer 1, the process workshops with Customer 2 were completed very quickly, and the work seemed to be easier. These workshops also helped prepare the participants for the policy workshops. After giving the CIA values to all of their processes, the participants had a better understanding of the possible issues in their operations and what might need to be addressed in the ISP. For example, one process had constant availability issues due to the system that was used, but these were never really addressed until their state was labeled red (in traffic lights evaluation) at a process workshop.

ISMcorp used the CMS system, which allowed for gathering and analyzing qualitative and quantitative information about the customer business and their wishes for the ISP. For example, the scores calculated from the CIA values worked as a basis for a risk assessment report that was completed before the actual policy workshops. Then again, the results of the policy workshop could be run as a report that is connected to the risk report. These reports worked as communication tools for the customers' managers.

Specifying learning

This cycle highlighted the importance of new CCs. The CC *strategy alignment* and CC *managers motivated* were included in the start-up meeting. This seemed to help in getting more people involved in the workshops. Individual process workshops for each unit also seemed to improve the flow of the work. Within the unit, people knew each others' work better and were able to evaluate whose work certain processes affect and who is responsible (CC *responsibility and authority*).

Project exit

The ISP projects with Customer 1 and Customer 2 had gaps of several months between the policy workshops and the end review. During this time, ISMcorp did not attract new customers to the ISP development service. After both customer projects had been finished, the researcher had one last discussion with the IS manager to end the AR project.

5.5 Changes related to critical considerations

This section summarizes the lessons learned from this AR project. CCs were developed in Cycles 1 and 2 and then used as catalysts for changes in the ISP development practice creation in Cycles 2, 3, and 4. The CCs summarize previous research literature into talking points that were used in the action-taking phases of the study. They steered the CDO and IS manager towards considering how understanding and assessing the situation happens in the ISP development. These are needed to guide the customers towards critical thinking from intuitive decision-making. This way, the CCs shifted the focus of the changes in ISP development from the general process steps towards improving their context-specific content.

The level of abstraction of the application of the CCs became more detailed in every cycle (see TABLE 6). In the first cycle, the abstraction level reflected the previous process-level approaches. The recommendations given to ISMcorp were quite high-level, with very little reference to the actual practice of implementing them. When the ISMcorp process was tested in Cycles 2–4, the researcher moved on to giving recommendations that were more closely linked to the actual practices carried out in the workshops. While the ISP development process was a consultancy service and, as such, was not unique to the organization creating the ISP, the IS manager thought that the process could be easily modified for different customers. For example, the starting meeting made it possible to adapt the number and participants of the workshops to the schedule of the project.

TABLE 6 Summary of the changes related to the CCs

Critical consideration	**Change during the AR project**
The organization's management is motivated to take action toward information security *CC management motivation*	Cycle 2: High-level management participated; attitudes "must get this fixed." Cycle 3: High-level management participated; middle-level voice commitment. Cycle 4: High-level management is encouraged to voice concerns about information security.
ISP is aligned with business strategy *CC strategy alignment*	Cycle 2: Strategy is included in the service process but not discussed in the testing. Cycle 3: Strategy is briefly discussed but not linked to the development. Cycle 4: Strategy is discussed by high-level management and linked to ISP development through business continuity.
ISP is defined in a way that is comprehensible to the organization members/subjects *CC: comprehensible documentation*	Cycle 3: Customer prefers less strict and defined rules to keep documentation and management processes simple. Cycle 4: Customer has difficulties in understanding ISO27002 requirements and how to change them into rules that apply to their work.
Understand the operational context of the ISP *CC: operational context*	Cycle 2: The process workshops revealed how much the organization adapts to its customers wishes. Cycle 3: Pressure from the partner company was one of the reasons for starting ISP development. Partners required their own documents. Cycle 4: Limited understanding of how widely information security affects communication with external stakeholders.
Stakeholder groups/people affected by the ISP are identified *CC stakeholders identified*	Cycle 2: Participating managers did know everyone the ISP would affect but did not consider the practicalities of changes in work routines. Cycle 3: Workshops included key persons by title but not all of them contributed to creating an ISP that would suit the working routines of their unit. Cycle 4: A wide range of employees from different business areas attended workshops, and clear connections with people's work and ISP were made.
Security requirements are determined at the company level *CC organization requirements*	Cycle 2: Difficulties in evaluating processes and identifying the most security critical operations. Cycle 3: Many areas in the ISP were chosen to have lower controls and higher accepted risk in order to avoid disrupting important processes.

continues

TABLE 6 continues

Critical consideration	**Change during the AR project**
ISP specifies the information affected by the policy *CC defines information*	Cycle 2: Instead of just identifying processes, a participant wanted to map the connections between the processes in order to visualize the flow of information in the organization. Cycle 4: Participants of the process workshops had difficulties in giving the CIA values to the processes. When describing their work, they could not identify the information they used in the processes they executed. The CIA evaluations focused heavily on personal information.
Authority and responsibilities are stated *CC authority & responsibility*	Cycle 2: During the process mapping workshops, each process was assigned an owner and key persons. These would be used to allocate responsibility for ISP implementation and monitoring. Cycle 3: The ISO27002-based ISP template required the definition of several inspection procedures for different parts of the policy. These were seen as redundant, and most were allocated to their information security officers. Cycle 4: Customer 2 had not previously named owners to their processes and allocating them made it clearer who should be contacted in case of security issues.
Indicators for compliance and goals are built into the ISP *CC indicators for goals*	Cycle 2: The CIA values are added to the process mapping workshops and they yield a report that allows a quick estimation of the most urgent needs for action. Cycle 3: Templates of compliance indicators were created and used at the end of the ISP development process to create ISP-specific indicators for the customer. Cycle 4: The customer had difficulty understanding the concepts behind CIA evaluations and applying them to the concept of information used in a process.
Information security development and maintenance are connected with the business processes *CC connected with processes*	Cycle 2: This CC was most valued by the CDO and was included in the ISP development process as a new step. In the internal test, the participants had trouble staying at the same abstraction level. Cycle 3: Customer 1 had only one process workshop, and the participants had trouble identifying processes since each business area was represented by only one or two people.
Policy is evaluated and tested in the organization *CC evaluating and testing*	Cycle 3: General metrics for monitoring ISP progress are planned and their selection with the customer is added in the review part at the end of the ISP process. The customer expects that evaluating an ISP will require too much work.

The 11 CCs are grouped here into three categories, which are analyzed in the following sections. The groups are as follows:

- Aligning the developed ISP to the context of the organization
    - *CC strategy alignment,*
    - *CC operational context,*
    - *CC organization requirements,*
    - *CC defines information,*

    - *CC connected with processes.*
- People and interpersonal dynamics
    - *CC management motivation,*
    - *CC stakeholders identified,*
    - *CC authority & responsibility.*
- Quality of the new rules
    - *CC comprehensible documentation,*
    - *CC indicators for goals,*
    - *CC evaluating and testing.*

5.5.1 Alignment with the organization

The alignment of ISP development with business requirements is highly recommended in the literature to avoid creating conflicting requirements for security and business. The CCs in this category encourage ISP developers to consider different aspects of their businesses and evaluate how IS issues might relate to them.

The only clear change in ISMcorp's process model for the ISP development service was how the business strategy was covered in the process. First, the strategy was mentioned only at the end of the process model, where it meant a high-level abstraction (executive summary) of the most important points of the ISP. This was changed so that the project start would include a discussion about the customer's business strategy and how that affects security goals. However, the IS manager said that this didn't really happen in the starting meetings since the customers didn't really have any formal strategies. He commented that all he could do was encourage them to think about business continuity and strategy.

For example, Customer 1 put quite a small weight on business strategy development. A manager commented, "I wonder if it is old-fashioned to contemplate such things that will never come true." The importance of strategies for an organization depends on its capabilities and the market in which it operates. Aligning an ISP with a strategy that does not steer the operations of the organization in reality is redundant. However, any planning that is put into action should be considered from an IS point of view to avoid conflicts in the future.

Customers 1 and 2 had several partners and subcontractors that were vital to their business operations. Customer 1 even said that an important partner had asked for an ISP declaration but had been left waiting since there wasn't any documentation to present. Dealing with the issue of extending the policy to cover partners was not straightforward. Not least because the policy workshops based on ISO27002 did not include a specific workshop for partnerships or collaboration; instead, Section 15.1 "Information security in supplier relationships" (Finnish Standards Association, 2014), was a small part of another workshop.

A large company in the center of its business network often has the ability to dictate rules for collaboration, and the same rules may be replicated throughout the ISPs of network members for convenience. A real-life example of this was given in an action planning workshop where Nokia's ISP was discussed and how, during the "golden age" (the early 2000s), it was replicated throughout the Finnish IT sector. It was agreed that this was not the direction ISMcorp wanted to develop their ISP service since they believed that adding actual security over compliance was the thing that would be most beneficial to them and their customers.

In a network of SMEs, there may not be a clear leader, and thus no easy way of determining who sets the rules. Regarding the question of sharing ISP documents with partners, a Customer 1 representative stated that any documentation for the partners should be a maximum of one page long if they hoped that the document would be read. The ISP should also be general enough that they do not need to update it every time they gain a new partner.

The ISP development workshops were based on the ISO27002 standard, which means that this external document played a big role in setting requirements for the policy. The IS manager said that neither of the customers thought that there was anything missing or not covered. On the contrary, the customers wondered if every area was really worth going through, such as encryption. The standard requires, for example, that management should state an approach to what information is encrypted, and encryption algorithms should be chosen based on the risk assessment (Finnish Standards Association, 2014). Making decisions like these requires an in-depth understanding of the threat environment, the sufficiency of alternative solutions, and the entirety of information assets. While the workshop participants would have some of this knowledge, the reality is that the subject is so complex that both customers ended up choosing the alternative that caused the least work—no encryption.

In the second cycle internal test, the CDO of ISMcorp mentioned that he preferred that their company only had critical and important processes and did not see why they would have any value-adding processes. This led to a situation in which most of the processes in the process map were marked as critical and only a few as value-adding. Although it is understandable that a company's operations are as lean as possible, this thinking led to a situation in which the process evaluation scale turned redundant. This is a situation in which the group would have benefited from first discussing how they see the scale intervals and how many critical processes there might be in total. At one point, a workshop participant commented, "This is extra critical," which is an indicator that their scale could have had even more than three categories.

One of the key reasons why the process workshops were added to the ISP development process was to instill IS-oriented thinking. The goal was that by starting to understand what role information plays in the processes of the company, the workshop participants would better understand how the decisions made in the policy workshops would affect these processes. The problems in including organization members in the ISP development may stem from the way people conceptualize the world around us. Often, the person who is given the responsibility of making the ISP is somehow educated in the field and may have knowledge of business management, information governance, or information technology. In the case of ISMcorp, both persons in charge of creating the ISP development method had a university master's degree in these fields. When planning the ISP development service, both the consultants and researchers were excited when they thought of including simple concepts, such as process thinking and the CIA triad, in the method. What they did not realize was that this way of conceptualizing work is not universal and might even be confusing for someone with a different background. This became evident at the process workshops at Customer 2, where each workshop consisted of only one business unit, and each workshop had different kinds of difficulties in identifying and assessing processes.

At the beginning of the policy workshops, the IS manager explained to the customers that the goal was to make a policy that would serve the business operations and that it was expected that a certain risk level would be tolerated in order to complement the business in the best possible way. Neither of the customers saw a need for a very strict policy. As one workshop participant jokingly put it, "If closing a million euro deal means we need to pay a big bribe to some big shot's nephew, then we'll do it." Although their policy did not end up condoning bribes, they chose to forego the strictest double checks recommended by the ISO standard.

These examples show how highlighting different aspects of the business context can help organization members better understand how different security rules can affect their operations. In many cases, the customer chose a lower-level security that was attainable and did not affect the operations too much. These kinds of compromises of the most good and least bad can be justified when ISP developers have a good enough understanding of the relevant facts about both business and IS needs.

5.5.2 People

The human factor is often referred to as the weakest link in IS. Therefore, many authors have recommended including different stakeholders in the ISP development process either as sources of information or actual developers. The CCs that relate to this theme represent the power structure of the organization (CC management motivation) and different groups who will be affected by the ISP in and outside the organization (CC stakeholders identified); in addition, they determine who has the right to make different IS decisions (CC authority & responsibility).

The main tool for motivating the high-level management in the ISMcorp ISP development process was the starting meeting, where the managers were invited and asked questions such as, "Why is information security important to this company at this time?" Since both customers were medium-sized companies, these high-level managers were also, to a great extent, the operational managers and, through those responsibilities, were involved in the other workshops as well.

The CDO explained that sometimes it is possible to start a project with only middle management (e.g., IS officer) support, but if high-level management does not come on board soon after the project starts, there may not be enough resources for the work, and the end result never achieves its goals. Efforts to motivate management should focus on the significance of IS to the organization and to the daily work of these people. The CDO explained how superficial motivation might be detrimental "even though in reality [managers] come along [to meetings], they can bluff interest to the organization. Probably at the same time, they are making service requests that are against all policies."

The significance of management motivation in the ISP development process depends on the size of the organization, organizational culture, leadership style (e.g., authoritarian, distributed), governance structure, etc. Whatever the circumstances, the policy development and implementation process will benefit if the managers are interested and ready to mandate actions. Motivation can also be superficial, such as the desire to look good in the eyes of an auditor or customer. While external influences may be good motivators, they may not be related to IS. Therefore, the ISP development service motivation effort included issues that highlighted how an ISP could lead to better outcomes for personnel and businesses.

Identifying internal stakeholders in the ISP became a central theme in the ISP development process, even though, in the first cycle, the idea did not get much traction. In the second cycle, the workshop participants were in such high places at ISMcorp that they described the company processes in an idealistic way and started to plan for improvements instead of describing the current situation. In the third cycle, the range of participants was wider, but the issue was that the workshops included all business areas, which meant that the participants became tired of listening to processes they knew nothing about. Any buy-in that had been built for the process would have deteriorated after a full-day workshop when the person's own expertise was needed only a few times. In the fourth round, the workshops were shorter and targeted at different business units, which meant that more people could participate, but still, the groups were small enough to include everyone in the conversation. After the fourth cycle, the IS manager thought that this issue could still be improved.

The IS manager wanted to improve the identification of the key persons (not necessarily the managers) who would be the center group throughout the process. He could then take better charge of how to use this group to benefit the process. For example, they could be invited to the project start meeting where the IS manager could start to build buy-in. They could be educated in understanding process thinking and information evaluation. In the longer run, this group could also play a significant role in implementation. The CDO envisioned the process to evolve into one where the consultants would act more as sparring partners, and the customer would learn how to do parts of the process themselves.

Authority and responsibilities were discussed in several parts of the ISP development process: First, in the process workshops, where the owners and key persons were written down for each process. Then, in the policy workshops, where responsibilities of different tasks, such as inspections, were decided. For both Customers 1 and 2, the employees often had several roles, and the hierarchies were low. For example, company owners may be both executives and carry out operational management at the same time. Customer 1 did not have an ISP, but they did have related roles and responsibilities stated in both quality and ICT documentation. Together, they did not, however, cover all areas of security. As the company grew, so did the need to cover security-related blind spots and make documented decisions on the responsibilities of monitoring processes and ISP areas.

The CCs relating to people approached the question of who is affected from different angles. They helped in changing the ISP development process into one where people from different parts of the organization were asked to share knowledge on how IS-related issues affect their work. The discussions also helped in understanding who was most affected by different decisions and what their preferences would be about implementing security measures, as well as in evaluating whose preferences should be met to select the best alternative for the business. However, this is a very complex task, and while the customers were able to do this evaluation in some cases, there were many parts of the ISP where they had trouble understanding how IS rules would affect employees.

5.5.3 Quality of the rules

It is important to manage the quality of the ISP and the development process to avoid problems after implementation. It should be clear what the ISP is trying to achieve and how its success can be evaluated (CC indicators for goals). The development process should also include some kind of evaluation of the created rules against the realities of work processes in the organization (CC evaluating and testing). The documentation of the policy must also be well executed to fit the communication style of the organization and to avoid issues of noncompliance that stem from poorly articulated rules (CC comprehensible documentation).

ISMcorp used the CRM system for documentation, which allowed for the inclusion of indicators and reports for different areas. In the process workshops, the first indicators were used when the participants evaluated the importance and CIA values of the processes. In the following policy workshop, the customers decided on inspections for different parts of the policy. Indicators were also added to the end of the ISP process in Cycle 3. The IS manager would suggest ways of implementing the policy and indicators that would fit the customer's ISP and could be monitored in the continuous security service. There were no indicators for strategy alignment, but the IS manager expected such issues to arise in the yearly inspections.

The ISP development process did not include any kind of testing as such. However, the last part of the process is the ISP review, in which the customer managers go through the policy and give comments. These meetings were held for both Customers 1 and 2 almost six months after the policy workshops. Regardless, these inspections went well, and the customers did not find anything major to change. In fact, the customers came into the last meeting with their own ideas on how the policy could be implemented and what needed to be changed. The IS manager expected that the actual testing would happen during the implementation and maintenance phases, and corrective measures could be decided upon in the reviews. However, this approach creates a significant time gap between detecting and fixing issues.

When planning Cycle 2, ISMcorp was presented with different approaches to ensure that the actual ISP text was something that the organization members would understand. The plan was to have comprehensive (several dozens of pages) documentation for the ISP, and different segments and guidelines would be targeted at different audiences. It was discussed whether the policy should be written by customers in their own words or if it would be better that the consultant would write the text and then teach the meaning to the customer. As having the customer as a part of the writing process seemed like too much work, ISMcorp decided on a compromise where the consultant would write the documentation, and at the end of the process, it would be reviewed and changed to fit the customer organization's communication style. However, the CDO commented that people's perceptions of things change over time, which is why continuous reviews are important, even if the text seems fine the first time it is written.

The quality-related CCs were put forth to try to ensure that the ISP development process would be as successful as possible. However, CC evaluating and testing and CC comprehensible documentation were the ones that had the least effect on designing the ISP development service. They were seen by ISMcorp as something that would be managed later in the ISP lifecycle. Then again, CC indicators for goals were present in several parts of the ISP development process, and several new indicators were developed during the AR project. The importance of these CCs lies in sharing an understanding of the success of the critical thinking that has happened during ISP development. They should help in comparing people's notions of the new rules and their usefulness in daily work.

Overall, we can see that each CC affected the ISP development process differently. With each of them, we can see how the thinking of the ISMcorp consultants changed from the first time they were presented with the CC toward the end of the project when they were implemented in the process. Working with the customers helped reveal any overly simplistic views about implementing the CCs and highlighted their importance. The CCs helped initiate critical thinking about ISP development and content in the areas that have been suggested to be relevant in previous research.

6 DISCUSSION

This dissertation has two main parts that answer the questions set out in the introduction. The first part analyzed the existing research contributions in ISP development in detail and provided answers to the question of *what kind of support and advice previous research literature provides for ISP development.* The second part introduced an AR project that focused on *how we can improve the practices of organization-specific ISP development.*

As an area of research, ISPs are not clearly defined. The definition depends on the organization or research project in question. This makes comparing research contributions rather cumbersome. Research on ISP development has also been conducted on several abstraction levels. On the highest level, research has focused on the relation of ISP to the steering of the entire organization or comparing several organizations. Most commonly, ISP development has been researched at the process level, in which common phases of assessment, development, implementation, and maintenance can be identified. Individual practices within these phases have, for example, been studied from the point of view of competing requirements for security and business. ISP developers have advice available in both research and best practice (standards and textbooks) literature. However, they often lack support in creating practices that include contextual factors, such as specific business needs.

In order to address the need for support for practices, an AR project was conducted to find solutions. In this study, ISP development was viewed as a series of decisions about new rules. The theory of critical thinking allowed us to understand better what kinds of phases a rulemaking process has. CCs were presented to connect the theory of critical thinking to previous research contributions and the practices of an ISP development project. They helped in considering the practices that must be in place for the project to be successful. These practices included ways of gathering relevant facts about the organization and understanding how organization members feel about the rules. This resulted in an ISP development process that created rules that were suited for the organization and had employee buy-in, even before moving to the implementation phase.

6.1 Main contributions

This research has focused on the details of ISP development practices rather than on generalizations of the process. Thus, the contributions of this study do not provide many recommendations for changes in higher-level ISP development methods that have been published before. However, the results of the study show how it may be problematic to enact the higher-level ideals of ISP development standards or methods in real life. The main contribution of this research is new knowledge on how ISPs are created in specific contexts, and it is further elaborated in the following five points (see TABLE 7).

TABLE 7 Main contributions

Contribution	Details
Elements of the definition of ISP	A description of the definitions and functions given to ISPs, their differences, and coverage
Abstraction levels	The distinction between research contributions on different levels and considering the connections between them
ISP development as a rulemaking process (theory of critical thinking)	The theoretical view of ISP development as a thought process that requires balancing between different requirements
Critical considerations	Identified points in ISP development that require critical thinking
Contextual view of the practices in ISP development	A detailed description on how higher-level concepts are carried out in practice and how context affects the way general guidelines are implementable

Researchers and practitioners have their own notions about the definitions and functions of ISPs. These include steering the organization, defining subjects and objects, and preparing for incidents. While this dissertation uses one definition of ISPs, it may only be useful for this study due to the dynamic nature of IS (von Solms, 2001). The contribution of defining the term exposes the plurality of the different aspects related to the term. Both researchers and practitioners who participated in the first cycle adopted very different views on what an ISP entails. Rather than trying to determine who is right, this work exposes the areas that must be agreed upon when discussing ISPs. This lays the groundwork for comparing ISP development efforts in different contexts, which is scarce in ISP development literature.

The linkages between different previous research contributions on ISPs are explained here through abstraction levels. While all abstraction levels of ISP research are linked in real-life situations, they are presented differently in research reports. A very common way to describe ISP development is through a lifecycle model (examples in FIGURE 1). This research has shown that while these models can help practitioners plan the ISP development process, they alone are not enough to ensure that the development process meets each organization's specific requirements. Without scrutinizing the level of abstraction or generalization of the advice, it is hard to detect gaps in the support needed for the ISP development process. This study resides on the lowest abstraction level where research contributions have focused on local practices, group dynamics, and conflicts between individual IS rules and business requirements (as in Burgemeestre et al., 2013; Hedström et al., 2011; E. Niemimaa & Niemimaa, 2017). This view extends, for example, the Security policy research framework (Cram et al., 2017) into a three-dimensional model where the connections of research contributions are not only linked in consecutive order but also on different levels. The three-dimensional view allows us to look for research gaps as well as take a critical look at the assumptions that are made when theorizing across levels. For example, much of the ISP development literature resides on the medium level, while ISP compliance is often studied on the lowest individual level.

Making ISPs is, at its core, a series of decisions regarding new rules. The theory of moral thinking (Hare, 1982) suggests that if the existing rule is not applicable to the situation (it is perceived to cause more harm than the alternative), the person might choose not to follow the rule. This implies that people trying to make good judgments about following rules and noncompliance with ISPs may stem from a bad rule, not necessarily a bad employee. The same idea has been discussed, and more research has been called for in IS and compliance literature (Cram et al., 2017; Siponen & Vartiainen, 2004). Therefore, the practices of making IS rules should have elements that enable policymakers to foresee the real-life situations in which the rules will be needed. In this way, the CCs steer the ISP developers away from intuitive thinking that expects that previous rules are applicable (copying rules from other organizations) without considering the context. Identifying situations that require moral reasoning has been called for by, for example, Myyry et al. (2009). The CCs created in this study are the link between Hare's theory and ISP research and practice.

The CCs guide the rule makers toward critical thinking through different aspects of the ISP. In this research, they were used as a tool to convert the contextual factors identified in previous research (see TABLE 3 and Appendix 2) into practices. Thus, this research answers the calls for studying how contextual factors are included in ISP development (Karlsson et al., 2017; Karyda et al. 2005). At the beginning of the AR project, the CCs were discussed on a higher abstraction level, but as the project moved forward, they were increasingly used to improve the practices in the ISP development process. The results of this study show that turning generalizations into local practices is a complex endeavor for both the IS expert and the organization's members. CCs are a way to help ISP developers move toward critical thinking by focusing on the facts of a particular context.

The empirical part of the study focused on understanding the ISP development process at its lowest level of abstraction. The major change that happened during the AR project in ISMcorp's ISP development process was the shift from using predetermined controls toward first understanding the information and security environment of the customer organization. While the ISO27002 controls were still used, the new practices in ISP development allowed the consultant and customer to share a deeper understanding of the significance of the controls in this context. This shows how the contextual factors identified in previous studies require the formation of practices that enable them. This detailed account of ISP development answers the calls for research that would explain how general guidelines are adopted in different contexts (Niemimaa & Niemimaa 2017).

6.2 Future research directions

In this dissertation, ISP development was studied through a qualitative analysis of the research literature and data from an AR study. Rather than focusing on the frequencies of the most popular topics or generalizing the most prominent practices, this research has also uncovered areas that have gained less attention previously and the detailed practices of ISP development in certain contexts. In general, future research directions in this area should critically examine the currently advocated approaches and focus on the assumptions behind them. Both qualitative and quantitative research is needed to gain a better understanding of what successful ISP development entails and how it is connected to improved IS.

Previous research is viewed here through abstraction levels to illustrate the differences and connections between approaches. Each of these abstraction levels is important and should be researched with data from different types of organizations. When designing these studies, researchers should be mindful of the different levels of abstraction and theorize accordingly. This work proposes three levels, but naturally, different approaches can be divided into any number of levels. Due to the differences in the units of study and the interest in the details of the situation, it may not be possible to carry theories through from one abstraction level to another. On the other hand, theories that connect these levels could bring new insights to the field of research. This approach sheds light on the different dimensions of ISP development advice that are (not) supported by research findings.

This research lays the groundwork for theorizing the connection between developing and complying with IS rules. Hare's (1982) theory, combined with the CCs, guides us in understanding how people create and choose the ISP rules they follow. Hare's (1982) theory considers critical thinking from the individual's point of view and addresses the possibility of insufficient information about the situation to make the best possible decision. Therefore, future research could investigate what effect creating rules for a specific context, compared to general IS rules, has on the effectiveness of the policy in protecting information assets. In the future, research is also needed to expose what kind of effect contextualized IS rules have on compliance. This requires being mindful of the unit of study (be it a process or an individual) in order to theorize the connection of ISP development to secure behavior.

In this study, the theory of critical thinking was used to explain the rulemaking process. However, this theory considers the moral thinking of an individual, while the focus of the study was to interpret how critical thinking guided the practices of the ISP developer group. From a theoretical point of view, this is not an issue since Hare (1982) states that moral thinking is something that we must do in concert with others (Hare, 1982, p. 228). Earlier research has suggested ways to resolve conflicts between different views (e.g., Burgemeestre et al., 2013; Hedström et al., 2011). However, further research is needed on how ISP developers comprehend and share information related to relevant facts and who is affected by ISPs. The data of this research project suggest that the workshop participants had very different notions of what the information was that they were protecting and how controls might affect people's work. There is a need to understand the mechanisms of knowledge sharing and how they affect the quality of ISPs.

6.3 Implications for practice

This study used a practice lens on ISP development with the aim of providing useful and important implications for the industry (Feldman & Orlikowski, 2011). The core message of this dissertation is that all the general guidelines put forth for ISP development need to be adapted for each development project. This may not be straightforward and requires attention to the IS needs of the organization. Understanding what kind of rules can be enforced and complied with in that context requires critical thinking. The developers need to find out the relevant facts and people who are affected by the new rules. This requires a significant amount of planning and information gathering before even getting to the formulation of the controls. However, it can be worth the effort since it can help solve issues of noncompliance and organization-specific IS threats before they come up in the maintenance phase. TABLE 8 includes questions related to each CC. They are similar to those asked by the researcher during the AR project.

TABLE 8 Questions to help the planning of ISP development practices

Critical consideration	**Have we planned a practice for…**
Management motivation	…creating understanding what issues motivate managers to improve information security? …improving managers' knowledge about the importance of information security? …getting a clear statement from the management for the mandate to develop a new ISP and the resources that are allocated to the work?
Alignment with business strategy	…creating understanding of what role information (security) plays in realizing the goals of the organization? …connecting the strategic planning and information security planning?
ISP is defined in a way that is comprehensible to the organization members/subjects	…translating general knowledge about information security threats to the organization context? …finding out what documentation style best works in this organization?
Understand the operational context of the ISP	…determining the sphere of operation for the ISP? …understanding how information flows in and out of the organization?
Stakeholder groups/people affected by the ISP are identified	…identifying whose work should be affected by the ISP? …asking opinions from those whose work is affected in and outside of the organization?
Security requirements are determined at the company level	…gathering information security requirements from the organization? …distinguishing between general requirements and threats and the ones that affect the information security of this organization?
ISP specifies the information affected by the policy	…identifying and organizing the information assets of the organization? …sharing understanding of what these specific assets are?
Authority and responsibilities are stated	…identifying who should have the power to do information security-related decisions for the organization? …defining the right balance between responsibilities and liberties?
Indicators for compliance and goals are built into the ISP	…formulating rules in a way that it is easy to determine if they are followed or not? …monitoring the change in information security in the organization and if it reaches the goals that have been stated in the ISP?
Information security development and maintenance are connected with the business processes	…identifying the most important functions of the organization and how information security is related to them? …initiating ISP development actions when changes or issues in the processes require them?
ISP evaluation and testing	…the organization members to give feedback on the contents? …testing how the new set of rules affects the work practices of the organization? … making adjustments in the content based on feedback before the ISP is deemed finished and approved?

There are many ways to find answers to these questions, and in this AR project, we discovered some good ways of doing so. We could call them "best practices," but we have only the comparison between cycles to determine what works and what does not (which might be quite common with things that are called "best practices"). In general, critical thinking in the rulemaking process requires a large amount of information, and the practices were improved to capture this information from the organization better. In this study, the leader of the ISP development project was a consultant, which affected how some practices were formed compared to an employee being mandated for the job. The fact that these were midsized companies with 100–200 employees also greatly affected the practices.

The kickoff meeting at the beginning of the ISP project has several important functions in terms of gathering knowledge about the situation. This is the meeting where people who have authority in the organization should mandate the ISP project to the people who have been given the responsibility of the project. These high-level managers should also be asked to explain why they thought IS was important to the organization. This is a way to scale the project and not exceed the mandate. As these midsized organizations may not have mature strategy processes in place, the first meeting is also where the ISP developer could try to interpret the management's goals for the organization and its IS. This step was missing in the first cycle, which then caused issues in the process workshops.

After the project has a mandate, ISP developers need to be chosen, and the project should be planned in more detail. Choosing many representatives around the organization helped in capturing the relevant facts about the situation. Cycles 2 and 3 only had unit leaders present, and they could not provide very detailed knowledge about the current state of the processes. In the last cycle, each unit was represented by several key persons, which led to a more comprehensive view of the processes and the state of IS. While these workshops concentrated on processes, they could have included more elements about identifying information assets and stakeholders (internal and external).

Choosing the development team is an important step in the development project, although it is rarely mentioned in the research literature. In critical thinking, there is a need to understand how people feel about the rules that are created. Without actively engaging organization members in the conversation, there is a danger of creating rules that people think cause more harm than good. This, again, leads to noncompliance or actions that may harm IS or business operations.

In this study, ISMcorp used the ISO27002 standard to create a template of an ISP that would then be adapted for each customer. At the beginning of the project, the general controls seemed sufficient for any organization. When the CCs were introduced and formed into practice, it became clear that the general controls needed a fair amount of adaptation to serve each organization well. We could view this as a change from intuitive thinking to critical thinking. This change is essential when there is a need to create rules that are perfectly suited for the context and protect the information assets of a specific organization. There is an abundant amount of best practice literature available for ISP development, but applying it may not lead to quality results if ISP developers are unable to question the underlying assumptions behind the advice and think critically about their suitability to the context.

7 CONCLUSION

This dissertation has provided a detailed account of ISP development research and studied the practice of adapting general guidelines to a specific context. The definition of ISP is not understood similarly across the field, but in this study, the term was used mainly for managerial policies that cover not only security goals but also the rules that are put in place to reach those goals in a specific organization. This rather broad definition of the term is reflected in the scope of what is considered ISP development in this study.

A bulk of previous research contributions to ISP development have studied the issue from a process-level point of view, generalizing commonalities between organizations. This study focused on the practices that happen within these higher-level processes. These practices are specific to the context and may not be generalized; rather, they illustrate how generalizations guide (or fail to guide) the real-life development process.

This study was based on the premise that the quality of the ISP rules affects how well they can be complied with and thus safeguard the organization's information assets. The theoretical basis of this thesis lies in Hare's (1982) theory of moral thinking. According to it, each of us engages in moral thinking when creating or following rules. If there does not seem to be a suitable rule one could follow without causing too much harm, one moves on to create a new rule for the situation. The empirical part of this study focused on the rulemaking process that would result in rules that would suit the contextual needs of the organization and thus diminish the need for employees to create their own rules to follow.

An ISP developer may have limited knowledge about the relevant facts of the organization and how employees feel about IS rules. This, again, may lead to intuitive thinking, where generic ISP guidelines are deemed adequate to safeguard the information assets of the organization. To promote practices that enhance the gathering of knowledge about the context, a set of CCs was created. They were used to help the ISP developers improve the development practices to ones that were able to create context-specific IS rules.

The findings of this study can guide practitioners in critically examining the way ISP rules are created and followed in their organizations. If rules are not created for a specific context, policy subjects may choose not to follow them. Therefore, the ISP development process should include practices that allow uncovering the relevant facts of the organization and how organization members view the potential new rules. The CCs put forth in this study can help in creating ISP development practices that support making rules that are easy to comply with and are thus effective in protecting the information assets of the organization.

YHTEENVETO (SUMMARY IN FINNISH)

Tietoturvapolitiikat (TTP:t) ovat keskeinen osa organisaatioiden tietoturvatoimintaa. Ne asettavat tavoitteita tiedon turvaamiselle ja ohjaavat työntekijöitä saavuttamaan nämä päämäärät. TTP ei ole terminä yksiselitteisesti määritelty ja sen käyttö tutkimuskirjallisuudessa ja organisaatioissa onkin varsin kirjavaa. Jotkin yleiset teemat kuitenkin toistuvat TTP:n ominaisuuksien ja toiminnan kuvauksissa. Sen oletetaan ohjaavan organisaatiota tavoitteiden ja sääntöjen kommunikoinnin kautta. Siinä määritellään sekä politiikan kohteena olevia toimijoita sekä tietovarannot, joita pyritään turvaamaan. Sen tarkoitus on myös valmistella organisaatiota käsittelemään riskejä ja palautumaan häiriötilanteista. Tässä väitöskirjassa TTP on määritelty koskemaan laajasti kaikkia organisaation tietoturvan tavoitteita ja ohjeita.

TTP:n kehitykselle on tarjottu ohjeita niin tutkimuskirjallisuudessa kuin käytännön oppaissakin. Yleinen lähestymistapa TTP:n kehitykseen ovat elinkaarimallit, joissa kuvataan syötteitä, kuten arvioinnit, TTP:n luominen sekä tuotosten laittaminen käytäntöön ja ylläpitäminen kunnes sykli alkaa taas alusta. Jokaisella organisaatiolla on kuitenkin sille ominaiset liiketoimintavaatimukset, joiden vuoksi on tarve suunnitella kehittäminen niin, että se tukee menetelmän ja syntyvän politiikan mukauttamisen kontekstiin. Tässä prosessissa luotujen sääntöjen tulee olla hyvin suunniteltuja, jotta työntekijöiden on mahdollista noudattaa niitä ilman, että ne ovat ristiriidassa heidän muiden velvollisuuksiensa kanssa.

Tässä väitöskirjassa esitellään TTP:n kehittämiseen liittyvä toimintatutkimus. Sen teoreettinen pohja rakentuu ajatukselle, että TTPn kohteena oleva henkilö käyttää moraalista ajattelua ja tekee päätöksiä sääntöjen noudattamisesta perustuen sille, mikä toiminta johtaisi parhaaseen lopputulokseen. Tämä vaikuttaa myös TTP:n kehittämisprosessiin. Politiikan kehittäjien on voitava kriittisesti arvioida vaihtoehtoja uusille säännöille perustuen heidän tietämykseensä organisaation toiminnasta. Tutkimusprojektissa tutkijat auttoivat konsulttiyritystä rakentamaan uudelleen heidän TTP:n kehittämispalvelunsa sellaiseksi, joka vastaa paremmin asiakasorganisaation tietoturvatarpeita. Jotta kriittistä ajattelua voitiin tukea kehittämisen aikana, kehitettiin 11 kriittistä näkökulmaa, jotka perustuivat aiemmalle tutkimukselle sekä yritysten esittämille tarpeille. Kriittisiksi näkökulmiksi valittiin sellaisia asioita TTP:n kehittämisessä, jotka tarvitsivat uusia käytäntöjä tukemaan kriittistä ajattelua. Toimintatutkimuksen neljän syklin aikana TTP:n kehittämisprosessiin luotiin uusia käytäntöjä, joilla voitiin parantaa asiakasorganisaatiossa faktojen sekä työntekijöiden mielipiteiden kartoitusta. Tämä mahdollisti sellaisten tietoturvasääntöjen valitsemisen, jotka sopivat yhteen yrityksen toiminnan kanssa.

Väitöskirjan alkuosa muodostuu laajasta kirjallisuuskatsauksesta, jossa tarkastellaan kriittisesti tietojärjestelmätieteen alan TTP:n kehityksen tutkimusta. Perusteellinen käsitemääritelmien analyysi jäsentää eri käsitteiden kirjoa ja helpottaa näin eri näkökulmien vertailua. Tutkimuskontribuutioiden vertailu eri abstraktiotasojen kautta taas auttaa ymmärtämään mihin TTP:n kehittämisen osiin on olemassa tutkimukseen pohjautuvaa tukea.

Tämä väitöskirja edistää nykyistä TTP:n kehittämisen tutkimusta esittämällä tavan muuntaa yleisiä ohjeita paikallisiksi käytännöiksi. Tutkimus perustui näkökulmalle TTP:sta sääntökokoelmana, jonka luomisessa käytetään moraalista ajattelua. Jotta politiikan tekijät käyttäisivät kriittistä ajattelua sääntöjä luodessaan, on heidän osattava kiinnittää huomiota organisaatiolle spesifisiin alueisiin. Tämän tukemiseksi esitettiin lista kriittisiä näkökulmia, joilla TTP:n kehittämisen paikallisia käytäntöjä voidaan tukea. Kriittisiä näkökulmia voidaan myös käyttää TTP:n kehityksen onnistumisen jatkotutkimukseen.

REFERENCES

Abrams, M., & Bailey, D. (1995). Abstraction and Refinement of Layered Security Policy. In M. D. Abrams, S. G. Jajodia, & H. J. Podell (Eds.), *Information Security-An integrated Collection of Essays* (pp. 126–136). IEEE Computer Society Press.

Abu-Musa, A. (2010). Information security governance in Saudi organizations: An empirical study. *Information Management and Computer Security*, *18*(4), 226–276. https://doi.org/10.1108/09685221011079180

Albrechtsen, E. (2007). A qualitative study on users' view on information security. *Computers & Security*, *26*(2007), 276–289. https://doi.org/10.1016/j.cose.2006.11.004

Anderson, R. J. (1996). A security policy model for clinical information systems. *Proceedings 1996 IEEE Symposium on Security and Privacy*, 30–43. https://doi.org/10.1109/SECPRI.1996.502667

Antón, A., & Earp, J. (2001). Strategies for Developing Policies and Requirements for Secure Electronic Commerce Systems. In A. K. Ghosh (Ed.), *Recent Advances in E-Commerce Security and Privacy* (pp. 29–46). Kluwer Academic Publishers.

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, *13*(4), 195–201. https://doi.org/10.1016/j.istr.2008.10.006

Balozian, P., & Leidner, D. (2017). Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory. *Data Base for Advances in Information Systems*, *48*(3), 11–43. https://doi.org/10.1145/3130515.3130518

Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems*, *1*(2), 121–130. https://link.springer.com/article/10.1057/ejis.1991.20

Baskerville, R. (1993). Information Systems Security Design Methods: Implications for Information Systems Development. ACM Computing Surveys, 25(4), 375–414. https://doi.org/10.1145/162124.162127

Baskerville, R. (1999). Investigating Information Systems with Action Research. *Communications of the Association for Information Systems*, *2*(3), 2–31. https://doi.org/10.17705/1CAIS.00219

Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, *15*(5/6), 337–346. https://doi.org/10.1108/09576050210447019

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, *51*(1), 138–151. https://doi.org/10.1016/j.im.2013.11.004

Baskerville, R., & Wood-Harper, A. (1998). Diversity in information systems action research methods. *European Journal of Information Systems*, *1998*(7), 90–107. https://doi.org/10.1057/palgrave.ejis.3000298

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.2307/25750690

Burgemeestre, B., Hulstijn, J., & Tan, Y.-H. H. (2013). Value-based argumentation for designing and auditing security measures. *Ethics and Information Technology*, *15*(3), 153–171. https://doi.org/10.1007/s10676-013-9325-2

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, *29*(3), 157–188. https://doi.org/10.2753/MIS0742-1222290305

Coles-Kemp, L. (2009). Information security management: An entangled research challenge. *Information Security Technical Report*, *14*(4), 181–185. https://doi.org/10.1016/j.istr.2010.04.005

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, *14*(4), 186–196. https://doi.org/10.1016/j.istr.2010.04.004

Corpuz, M. S. (2011). The Enterprise Information Security Policy as a Strategic Business Policy within the Corporate Strategic Plan. *The 8th International Symposium on Risk Management and Cyber-Informatics: RMCI 2011*, 275–279.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, *26*(6), 605–641. https://doi.org/10.1057/s41303-017-0059-9

da Veiga, A., & Eloff, J. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

D'Arcy, J., & Hovav, A. (2007). Deterring Internal Information Systems Misuse. *Communications of the ACM*, *50*(10), 113–117. https://doi.org/10.1145/1290958.1290971

D'Aubeterre, F., Singh, R., Iyer, L., D 'aubeterre, F., Singh, R., & Iyer, L. (2008). Secure activity resource coordination: empirical evidence of enhanced security awareness in designing secure business processes. *European Journal of Information Systems*, *17*(5), 528–542. https://doi.org/10.1057/ejis.2008.42

Davison, R. M., Martinsons, M. G., & Kock, N. (2004). Principles of canonical action research. *Information Systems Journal*, *14*(1), 65–86. https://doi.org/10.1111/J.1365-2575.2004.00162.X

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, *2001*(11), 127–153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information Systems Journal*, *16*, 293–314. https://doi.org/10.1111/j.1365-2575.2006.00219.x

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, *29*(6), 449–457. https://doi.org/10.1016/j.ijinfomgt.2009.05.003

Doherty, N. F., & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis. *Information Resources Management Journal*, *18*(4), 21–39. https://doi.org/10.4018/irmj.2005100102

Feldman, M. S., & Orlikowski, W. J. (2011). Theorizing practice and practicing theory. *Organization Science*, *22*(5), 1240–1253. https://doi.org/10.1287/ORSC.1100.0612

Finnish Standards Association. (2014). *SFS-ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls* (p. 183). Finnish Standards Association.

Flowerday, S. v, & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*(2016), 169–183. https://doi.org/10.1016/j.cose.2016.06.002

Galletta, D. F., & Hufnagel, E. M. (1992). A model of end-user computing policy: Context, process, content and compliance. *Information & Management*, *22*(1), 1–18. https://doi.org/10.1016/0378-7206(92)90002-W

Glasgow, J., Macewen, G., & Panangaden, P. (1992). A Logic for Reasoning about Security. *ACM Transactions on Computer System*, *10*(3), 226–264.

Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. *Journal of Strategic Information Systems*, *19*(4), 281–295. https://doi.org/10.1016/j.jsis.2010.10.002

Gritzalis, D. (1997). A baseline security policy for distributed healthcare information systems. *Computers & Security*, *16*(8), 709–719.

Haag, S., Siponen, M., & Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. *The DATA BASE for Advances in Information Systems*, *52*(2), 25–67. https://doi.org/10.1145/3462766.3462770

Hantrais, L., Allin, P., Kritikos, M., Sogomonjan, M., Anand, P. B., Livingstone, S., Williams, M., & Innes, M. (2020). Covid-19 and the digital revolution. *Journal of the Academy of Social Sciences*, *16*(2), 256–270. https://doi.org/10.1080/21582041.2020.1833234

Hare, R. M. (1982). *Moral thinking : its levels, method, and point*. Oxford University Press. http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=728892

Haworth, D., & Pietron, L. (2006). Sarbanes–Oxley: Achieving Compliance By Starting With Iso 17799. *Information Systems Management*, *23*(1), 73–87. https://doi.org/10.1201/1078.10580530/45769.23.1.20061201/91775.9

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems*, *20*(4), 373–384. https://doi.org/10.1016/j.jsis.2011.06.001

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers*, *2019*(21). https://doi.org/10.1007/s10796-019-09959-1

Heikka, J. (2008). A Constructive Approach to Information Systems Security Training: An Action Research Experience. *AMCIS 2009 Proceedings*, 1–8. https://aisel.aisnet.org/amcis2008/319

Höne, K., & Eloff, J. (2002). Information security policy — what do international information security standards say? *Computers & Security*, *21*(5), 402–409. https://doi.org/10.1016/S0167-4048(02)00504-7

Howard, P. (2002). The Security Policy Life Cycle: Functions and Responsibilities. In H. Tipton & M. Krause (Eds.), *Information Security Management Handbook* (pp. 377–388). Auerbach Publications. https://doi.org/10.1201/9781351073547

Hsu, C. (2009). Frame misalignment: Interpreting the implementation of information systems security certification in an organization. *European Journal of Information Systems*, *18*(2), 140–150. https://doi.org/10.1057/ejis.2009.7

Iivari, J., & Venable, J. (2009). Action research and design science research - Seemingly similar but decisively dissimilar. *ECIS 2009 Proceedings*, *1*. https://aisel.aisnet.org/ecis2009/73

Jiang, H., Siponen, M., & Tsohou, A. (2021). Personal use of technology at work: a literature review and a theoretical model for understanding how it affects employee job performance. *European Journal of Information Systems*, 1–15. https://doi.org/10.1080/0960085X.2021.1963193

Karjalainen, M., & Siponen, M. (2011). Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches. *Journal of the Association for Information Systems*, *12*(8), 518–555. https://doi.org/10.17705/1jais.00274

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers and Security*, *67*. https://doi.org/10.1016/j.cose.2016.12.012

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers & Security*, *24*(3), 246–260. https://doi.org/10.1016/j.cose.2004.08.011

Kinnunen, H. (2017). Critical Considerations for Organisation-specific Information Security Policy Development. *Proceedings of the International Conference on Transformations and Innovations in Management*. https://doi.org/10.2991/ictim-17.2017.53

Kinnunen, H., & Siponen, M. (2018). Developing Organization-Specific Information Security Policies. *PACIS 2018 Proceedings*. https://aisel.aisnet.org/pacis2018/244/

Klaic, A. (2010). Overview of the state and trends in the contemporary information security policy and information security management methodologies. *Proceedings of the 33rd International Convention MIPRO*, 1203–1208.

Klaic, A., & Hadjina, N. (2011). Methods and tools for the development of information security policy — A comparative literature review. *Proceedings of the 34th International Convention MIPRO*, 1532–1537.

Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, *23*(1), 67–94. https://doi.org/10.2307/249410

Knapp, K., Morris, F., Marshall, T., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, *28*(7), 493–508. https://doi.org/10.1016/j.cose.2009.07.001

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. *Journal of Strategic Information Systems*, *26*(1), 39–57. https://doi.org/10.1016/j.jsis.2016.08.005

Lapke, M., & Dhillon, G. (2008). Power Relationships in Information Systems Security Policy Formulation and Implementation. *ECIS 2008 Proceedings*. https://aisel.aisnet.org/ecis2008/119

Levy, Y., & Ellis, T. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science: International Journal of an Emerging Transdiscipline*, *9*, 181–212. https://doi.org/10.28945/479

Li, H., Sarathy, R., Zhang, J., & Luo, X. (2014). Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal*, *2014*(24), 479–502. https://doi.org/10.1111/isj.12037

Lindup, K. (1995). A new model for information security policies. *Computers & Security*, *14*(8), 691–695.

Lopes, I., & Sá-Soares, F. (2010). Information Systems Security Policies: a Survey in Portugese Public administration. *Proceedings of the International Conference Information Systems (IADIS)*, 61–69.

Maynard, S. B., Ruighaver, A. B., & Ahmad, A. (2011). Stakeholders in Security Policy Development. *Proceedings of the 9th Australian Information Security Management Conference*, 182–188. https://doi.org/10.4225/75/57b546fecd8c6

McFadzean, E., Ezingeard, J.-N., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review*, *31*(5), 622–660. https://doi.org/10.1108/14684520710832333

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, *42*(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853

Morgan, S. (2022, January 19). *2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics*. Cybercrime Magazine. https://cybersecurityventures.com/cybersecurity-almanac-2022/

Myers, M., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information & Organization*, *17*(1), 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126–139. https://doi.org/10.1057/ejis.2009.10

Niemimaa, E. (2016a). A practice lens for understanding the organizational and social challenges of information security management. *PACIS 2016 Proceedings*. https://aisel.aisnet.org/pacis2016/58

Niemimaa, E. (2016b). Crafting an Information Security Policy: Insights from an Ethnographic Study. *ICIS 2016 Proceedings*, 1–16. https://aisel.aisnet.org/icis2016/Practice-OrientedResearch/Presentations/6

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems*, *26*(1), 1–20. https://doi.org/10.1057/s41303-016-0025-y

Niemimaa, M., & Niemimaa, E. (2019). Abductive innovations in information security policy development: an ethnographic study. *European Journal of Information Systems*, *28*(5), 566–589. https://doi.org/10.1080/0960085X.2019.1624141

Olnes, J. (1994). Development of security policies. *Computers & Security*, *13*(8), 628–636.

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, *88*(1), 1–14. https://doi.org/10.1016/j.cose.2019.101608

Posey, C., & Shoss, M. (2022, January 20). Research: Why Employees Violate Cybersecurity Policies. *Harward Business Review*.

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638–646. https://doi.org/10.1016/j.cose.2004.10.006

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly: Management Information Systems*, *34*(4), 757–778. https://doi.org/10.2307/25750704

Raggard, B. (2010). *Information Security Management: concepts and practice*. Taylor & Francis group.

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: A Policy Framework for Information Security. *Communications of the ACM*, *46*(7), 101–106. https://doi.org/10.1145/792704.792706

Safa, N. S., & von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451. https://doi.org/10.1016/j.chb.2015.12.037

Saleh, M. (2011). Information Security Maturity Model. *International Journal of Computer Science and Security*, *5*(3), 316–337.

Sandhu, R. S., & Samarati, P. (1994). Access control: principle and practice. *IEEE Communications Magazine*, *32*(9), 40–48. https://doi.org/10.1109/35.312842

Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security*, *22*(3), 279–308. https://doi.org/10.1108/IMCS-05-2013-0041

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. https://doi.org/10.1108/09685220010371394

Siponen, M. (2005). An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems*, *14*(3), 303–315. https://doi.org/10.1057/palgrave.ejis.3000537

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, *49*(8), 97–100. https://doi.org/10.1145/1145287.1145316

Siponen, M., & Baskerville, R. (2018). Intervention effect rates as a path to research relevance: Information systems security example. *Journal of the Association for Information Systems*, *19*(4), 247–265. https://doi.org/10.17705/1jais.00491

Siponen, M., & Iivari, J. (2006). Six Design Theories for IS Security Policies and Guidelines. *Journal of the Association for Information Systems*, *7*(7), 445–473. https://doi.org/10.17705/1jais.00095

Siponen, M., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *The Data Base for Advances in Information Systems*, *38*(1), 60–80. https://doi.org/10.1145/1216218.1216224

Siponen, M., Soliman, W., & Vance, A. (2022). Common Misunderstandings of Deterrence Theory in Information Systems Research and Future Research Directions. *Data Base for Advances in Information Systems*, *53*(1), 25–60. https://doi.org/10.1145/3514097.3514101

Siponen, M., & Vartiainen, T. (2004). Unauthorized copying of software and levels of moral development: A literature analysis and its implications for research and practice. *Information Systems Journal*, *14*(4), 387–407. https://doi.org/10.1111/j.1365-2575.2004.00179.x

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

Solms, B. von, & von Solms, B. (2001). Information security - A multidimensional discipline. *Computers & Security*, *20*(6), 504–508. https://doi.org/10.1016/S0167-4048(01)00608-3

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, *22*(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Sterne, D. F. (1991). On the buzzword "security policy." *Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy*, 219–230. https://doi.org/10.1109/RISP.1991.130789

Straub, D. (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, *1*(3), 255–276. https://doi.org/10.1287/isre.1.3.255

Talbot, S., & Woodward, A. (2009). Improving an organisations existing information technology policy to increase security. *Proceedings of the 7th Australian Information Security Management Conference*, 120–128. https://doi.org/10.4225/75/57b416db30df3

Trček, D. (2003). An integral framework for information systems security management. *Computers & Security*, *22*(4), 337–360. https://doi.org/10.1016/S0167-4048(03)00413-9

Trompeter, C. M., & Eloff, J. H. P. (2001). A Framework for the Implementation of Socio-ethical Controls in Information Security. *Computers & Security*, *20*(5), 384–391. https://doi.org/10.1016/S0167-4048(01)00507-7

Tuyikeze, T., & Flowerday, S. v. (2014). Information Security Policy Development and Implementation: A Content Analysis Approach. *Proceedings of the Eight International Symposium on Human Aspects of Information Security & Assurance (HAISA 2014)*, 11–20.

Tuyikeze, T., & Pottas, D. (2010). An Information Security Policy Development Life Cycle. *Proceedings of the South African Information Security Multi-Conference (SAISMC 2010)*, 165–176.

Vance, A., & Siponen, M. (2012). IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing*, *24*(1), 21–41. https://doi.org/10.4018/joeuc.2012010102

von Solms, R., Thomson, K.-L., & Maninjwa, P. M. (2011). Information Security Governance control through comprehensive policy architectures. *Proceedings of the Information Security South Africa (ISSA 2011)*, 1–6. https://doi.org/10.1109/ISSA.2011.6027522

Ward, P., & Smith, C. (2002). The Development of Access Control Policies for Information Technology Systems. *Computers & Security*, *21*(4), 356–371. https://doi.org/10.1016/S0167-4048(02)00414-5

Whitman, E. M. (2008). Security Policy: from design to maintenance. In R. Baskerville, D. W. Straub, & S. E. Goodman (Eds.), *Information Security: Policy, Processes, and Practices* (pp. 123–151). Routledge.

Wood, C. (1995). Writing InfoSec Policies. *Computers & Security*, *14*, 667–674. https://doi.org/10.1016/0167-4048(96)81706-8

Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, *31*(4), 360–365. https://doi.org/10.1016/j.ijinfomgt.2010.10.006

APPENDIX 1. SCOPUS SEARCH TERM

```
EXACTSRCTITLE ( “European Journal of Information Systems” )
OR EXACTSRCTITLE ( “Information Systems Journal” )
OR EXACTSRCTITLE ( “Information Systems Research”)
OR EXACTSRCTITLE ( “association of IS” )
OR EXACTSRCTITLE ( “Journal of MIS” )
OR EXACTSRCTITLE ( “Journal of Strategic Information Systems” )
OR EXACTSRCTITLE ( “MIS Quarterly” )
OR EXACTSRCTITLE ( “Communications of the association for information systems” )
OR EXACTSRCTITLE ( “Information and management” )
OR EXACTSRCTITLE ( “Data Base for Advances in Information Systems”)
OR EXACTSRCTITLE ( “Information management and computer security” )
OR EXACTSRCTITLE ( “Computers and security” )
AND TITLE-ABS-KEY ( “security policy” )
AND TITLE-ABS-KEY (develop*)
OR TITLE-ABS-KEY (creat*)
OR TITLE-ABS-KEY (formula*)
OR TITLE-ABS-KEY (method*)
```

APPENDIX 2. LITERATURE ON CRITICAL CONSIDERATIONS

Table 9 contains references to the research articles that discuss the themes of critical considerations. Adapted from the article by Kinnunen (2017).

TABLE 9 Critical considerations in the research literature

Critical consideration	Literature mention
The organization's management is motivated to take action toward information security	Ashenden, 2008; Knapp et al., 2009; B. von Solms & von Solms, 2001; Trček, 2003; Wood, 1995
ISP is aligned with business strategy	Burgemeestre et al., 2013; Coles-Kemp, 2009; Galletta & Hufnagel, 1992; Lopes & Sá-Soares, 2010; Posthumus & von Solms, 2004; Rees et al., 2003; R. von Solms et al., 2011
ISP is defined in a way that is comprehensible to the organization members/subjects	Chen et al., 2012; Flowerday & Tuyikeze, 2016; Hedström et al., 2011; Lopes & Sá-Soares, 2010; Myyry et al., 2009
Understand the operational context of the ISP	Ashenden, 2008; Flowerday & Tuyikeze, 2016; Olnes, 1994; Rees et al., 2003; B. von Solms & von Solms, 2001; Wood, 1995
Stakeholder groups/people affected by the ISP are identified	Ashenden, 2008; Baskerville & Siponen, 2002; Burgemeestre et al., 2013; Flowerday & Tuyikeze, 2016; M. Niemimaa & Niemimaa, 2019; Olnes, 1994; Posthumus & von Solms, 2004; C. M. Trompeter & Eloff, 2001
Security requirements are determined at the company level	Baskerville & Siponen, 2002; Burgemeestre et al., 2013; D'Aubeterre et al., 2008; Flowerday & Tuyikeze, 2016; Karyda et al., 2005; Knapp et al., 2009; Lopes & Sá-Soares, 2010; Olnes, 1994; Posthumus & von Solms, 2004; Rees et al., 2003; R. von Solms et al., 2011; Wood, 1995
ISP specifies the information affected by the policy	Baskerville & Siponen, 2002; Lopes & Sá-Soares, 2010; Posthumus & von Solms, 2004; Rees et al., 2003; Silic & Back, 2014
Authority and responsibilities are stated	Baskerville & Siponen, 2002; Bulgurcu et al., 2010; Chen et al., 2012; Coles-Kemp, 2009; Olnes, 1994; C. M. Trompeter & Eloff, 2001; Wood, 1995
Indicators for compliance and goals are built into the ISP	Baskerville & Siponen, 2002; Höne & Eloff, 2002; B. von Solms & von Solms, 2001; R. von Solms et al., 2011
Information security development and maintenance are connected with the business processes	Baskerville & Siponen, 2002; D'Aubeterre et al., 2008; Galletta & Hufnagel, 1992; McFadzean et al., 2007; Posthumus & von Solms, 2004
Policy is evaluated and tested in the organization	Baskerville & Siponen, 2002; Olnes, 1994; Rees et al., 2003; Talbot & Woodward, 2009

APPENDIX 3. AR EVALUATION

Table 10 lists the principles for canonical action research (CAR) (Davison et al., 2004) and answers to the evaluation questions. While this dissertation adapted the CAR method for its own purposes, the questions are still useful for evaluating the research approach and reporting.

TABLE 10 Action research evaluation criteria

1. Criteria for the client-researcher-agreement (Davison et al., 2004, p. 70)	
1a Did both the researcher and the client agree that CAR was the appropriate approach for the organizational situation?	The research method was agreed upon when the researchers and ISMcorp applied for joint project funding.
1b Was the focus of the research project specified clearly and explicitly?	The research topic of ISP development was agreed, not the specifics of what the outcome would be.
1c Did the client make an explicit commitment to the project?	Client signed the project application and NDA; commitment was repeated verbally as the project started.
1d Were the roles and responsibilities of the researcher and client organization members specified explicitly?	Both the sides brought new people into the project in the beginning (author & IS manager), as the project continued their roles became clearer. In the action planning and evaluation phases, the researcher will take an active role in improving the ISP service. In the action-taking phase, the researcher would only observe, and the IS manager would enact the plans.
1e Were project objectives and evaluation measures specified explicitly?	Project objectives were discussed in the beginning. The evaluation was planned to be made through the testing of the ISP service.
1f Were the data collection and analysis methods specified explicitly?	Researcher informed about audio recording each time, and ISMcorp and customers allowed for the use of the transcribed data.
2. Criteria for the CAR process model (Davison et al., 2004, p. 72)	
2a Did the project follow the CPM or justify any deviation from it?	The process model was followed in Cycles 1 and 2, but in Cycles 3 and 4, the diagnosis and action taking were done in the same meetings.
2b Did the researcher conduct an independent diagnosis of the organizational situation?	Researcher reflected the situation against ISP literature and in later cycles against the CCs.
2c Were the planned actions based explicitly on the results of the diagnosis?	In the first cycle, the action planning was done solely on the basis of researcher's diagnosis. In later cycles, action planning was done based on the issues identified after the previous cycles and the CCs.

2d Were the planned actions implemented and evaluated?	The researchers plan was put into action in meetings with ISMcorp. The IS manager would be in charge of implementing the actions in practice. The researcher did not take part in actually facilitating the workshops where the altered process was tested/evaluated.
2e Did the researcher reflect on the outcomes of the intervention?	Researcher reflected on how the CCs were reflected in practice and if something different should have been done to improve the action.
2f Was this reflection followed by an explicit decision on whether or not to proceed through an additional process cycle?	After each evaluation and reflection, there were still clear issues that could be tackled in another cycle. After the last cycle the all bigger issues had been tackled.
2g Were both the exit of the researcher and the conclusion of the project due to either the project objectives being met or some other clearly articulated justification?	The project objectives were somewhat met since the minimum requirement was to improve the ISP development service and test it. The number of cycles was determined by the fact that ISMcorp had only two customers for the service at the time.
3. Criteria for the Principle of Theory (Davison et al., 2004, p. 74)	
3a Were the project activities guided by a theory or set of theories?	The project activities were guided by the theory of critical thinking and the CCs which were created during the project.
3b Was the domain of investigation, and the specific problem setting, relevant and significant to the interests of the researcher's community of peers as well as the client?	The project set out to tackle some of the problems identified in ISP development research literature. ISMcorp (and the other companies in Cycle 1) identified a need for practical solutions to develop ISPs.
3c Was a theoretically based model used to derive the causes of the observed problem?	The theory of critical thinking was used to understand the process of rulemaking. A testable model was not used. The CCs made it apparent that support for creating practices was needed.
3d Did the planned intervention follow from this theoretically based model?	The CCs were created in the action planning in order to aid in improving the rulemaking practices.
3e Was the guiding theory, or any other theory, used to evaluate the outcomes of the intervention?	The CCs were used as a basis of discussion when evaluating the intervention with ISMcorp.
4. Criteria for the Principle of Change through Action (Davison et al., 2004, p. 75)	
4a Were both the researcher and client motivated to improve the situation?	Both were keen to create a good ISP development service, but the idea of how this could be done was clarified to both during the project.
4b Were the problem and its hypothesized cause(s) specified as a result of the diagnosis?	Before the first cycle, the researcher was only partially aware of the causes of the problems. The diagnosis phases in the later cycles were better able to specify the problem.
4c Were the planned actions designed to address the hypothesized cause(s)?	Suggestions on how to fix the problems were planned based on the CCs

4d Did the client approve the planned actions before they were implemented?	Researcher only made suggestions while the client implemented the actual changes. The researcher did not act as a consultant but instead only observed the testing
4e Was the organization situation assessed comprehensively both before and after the intervention	The situation of the ISP development service was assessed with the CDO and IS manager, and their views were further assessed by the researcher.
4f Were the timing and nature of the actions taken clearly and completely documented?	All ISMcorp interviews and customer workshops were audio-recorded and notes were taken.
5. Criteria for the Principle of Learning through Reflection (Davison et al., 2004, p. 77)	
5a Did the researcher provide progress reports to the client and organizational members?	The researcher would contact the client any time there were new things that could be tried. The researcher did not make any changes independently.
5b Did both the researcher and the client reflect upon the outcomes of the project?	The researcher and the client had several meetings where the changes in the ISP development service were discussed. In the last meeting all changes were reflected on.
5c Were the research activities and outcomes reported clearly and completely?	All research activities were reported and the completeness of the account could be verified from the transcribed recordings.
5d Were the results considered in terms of implications for further action in this situation?	The (initial) analysis of the results was always done with the intention to find possible new suggestions to improve the ISP development process.
5e Were the results considered in terms of implications for action to be taken in related research domains?	Implications for future research were discussed in terms of theorizing on several abstraction levels.
5f Were the results considered in terms of implications for the research community (general knowledge, informing/re-informing theory)?	Hare's theory was introduced and used to illustrate the problematic background assumptions of user as the sole source of compliance issues. Lack of support for creating ISP development practices was discussed through the CCs.
5g Were the results considered in terms of the general applicability of CAR?	Action research was considered suitable for this kind of study that sought to solve industry problems with researcher intervention. Some issues with the researcher's participation were noted.