Received 24 March 2022
Revised 13 May 2022
Accepted 18 May 2022

The influence of inputs in the information security policy development: an institutional perspective

Lovisa Göransson Ording and Shang Gao
Department of Informatics, Örebro University, Örebro, Sweden, and
Weifeng Chen
Brunel Business School, Brunel University London, Uxbridge, UK

Abstract

Purpose – The purpose of this paper is to investigate what role literature-based inputs have on the information security policy (ISP) development in practice.

Design/methodology/approach – A literature review is carried out to identify commonly used inputs for ISP development in theory firstly. Secondly, through the lens of institutional theory, an interpretive approach is adapted to study the influence of literature-based inputs in the ISP development in practice. Semi-structured interviews with senior experienced information security officers and managers from the public sector in Sweden are carried out for this research.

Findings – According to the literature review, 10 inputs for ISP development have been identified. The results from the interviews indicate that the role inputs have on the ISP development serves as more than a rational tool, where organisational context, institutional pressures and the search for legitimacy play an important role.

Research limitations/implications – From the institutional perspective, this study signifies the influence of inputs on ISP development can be derived from institutionalised rules or practices established by higher authorities; actions and practices that are perceived as successful and often used by other organisations; the beliefs of what is viewed as appropriate to meet the specific pressures from stakeholders.

Practical implications – This research recommends five practical implications for practitioners working with the ISP development. These recommendations aim to create an understanding of how an ISP could be developed, considering more than the rational functionalist perspective.

Originality/value – To the best of the authors' knowledge, it is the first of its kind in examining the role of literature-based inputs in ISP development in practice through the lens of institutional theory.

Keywords Information security policy development, Information security, Inputs, Institutional theory, Social-organisational perspective

Paper type Research paper

Transforming Government: People, Process and Policy
Vol. 16 No. 4, 2022
pp. 418-435
Emerald Publishing Limited
1750-6166
DOI 10.1108/TG-03-2022-0030

1. Introduction

Information security policy (ISP) can be viewed as one of the key elements to having effective information security (InfoSec) (Doherty *et al.*, 2009; Höne and Eloff, 2002). Whitman (2008) defined ISP as "established rules that guide the protection of an organisation's assets". Goel and Chengalur-Smith (2010) defined ISP as:

> A document that states how an organisation plans to protect its information assets from external and internal threats, operationalises the implementation of security, and provides guidelines for employee and management conduct.

The ISP development process could be viewed as a logic model consisting of three phases (i.e. input, development and output) (Karyda *et al.*, 2005; Paananen *et al.*, 2020). The input phase includes the factors affecting the development phase of the ISP development, which further will result in a specific outcome. Cram *et al.* (2017) indicated that the majority of research within the ISP field tended to focus on ISP compliance, defined as the output. Moreover, several approaches are covered by the literature when describing and analysing the development process of an ISP (Flowerday and Tuyikeze, 2016; Karyda *et al.*, 2005; Knapp *et al.*, 2009; Rees *et al.*, 2003). However, analysing the problem from the input phase has not yet been explored extensively. For instance, how input flows and is translated into the development and output phase is critical to understand, as it might lead to issues in implementation and maintenance (Paananen *et al.*, 2020).

Furthermore, previous studies (Cram *et al.*, 2017; Flowerday and Tuyikeze, 2016; Karyda *et al.*, 2005; Knapp *et al.*, 2009; Paananen *et al.*, 2020) acknowledged the importance of knowing what inputs (e.g. standards, regulations) to use, and how to use them. However, there is a need to challenge these assumptions to gain an understanding of the difference between theory practice and the real practice of creating an ISP. For instance, Paananen *et al.* (2020) conclude in their analysis of ISP development phases that gaps exist between theory and practice. However, there are only a few studies that investigate the entire ISP development process in practice by comparing an espoused theory (Niemimaa and Niemimaa, 2019). The literature mentions many examples of different sources that should be used as inputs. However, there is a gap in the research on identifying how these suggested literature-based inputs actually influence the ISP development process in practice (Cram *et al.*, 2017; Paananen *et al.*, 2020).

The objective of the study is to investigate what role literature-based inputs have on ISP development in practice. An interpretive approach by using institutional theory is applied to investigate if institutional forces can describe the problem of insufficient ISPs in organisations. This study aims to provide a new perspective on what role do literature-based inputs play to influence ISP development in practice. The following two research questions (*RQ*) have been developed accordingly:

RQ1. What are the commonly used inputs for ISP development?

RQ2. What role do literature-based inputs play to influence the ISP development process in practice?

Senior information security officers and managers from Sweden have been selected as the subjects to address *RQ2*. According to the Global Cybersecurity Index 2020 report from International Telecommunication Union, Sweden ranks 26th worldwide with a high cybersecurity commitment.

The rest of the paper is organised as follows. Section 2 describes the theoretical background. Section 3 illustrates a research model on inputs for ISP development. A study

on the influence of inputs on the ISP development process is described in Section 4. The results from the conducted interviews are presented and analysed in Section 5. Finally, discussion and conclusion of this study are provided in Section 6.

2. Theoretical background

2.1 Information security policy development process

Developing an ISP is the first step towards preparing organisations for threats and vulnerabilities that are associated with InfoSec (Whitman, 2008). However, how to develop an ISP lacks one general approach. It is instead found that several approaches exist in the literature. Figure 1 presents the five previously discussed studies (Rees *et al.*, 2003; Whitman, 2008; Karyda *et al.*, 2005; Knapp *et al.*, 2009; Flowerday and Tuyikeze, 2016) on ISP development processes in a phase-oriented graphical overview. Three classified phases are input, development and output.

The output of the ISP development is widely studied from the awareness and compliance point of view (Paananen *et al.*, 2020; Chen *et al.*, 2021; Khando *et al.*, 2021). However, the input phase of the ISP development needs to be further explored. The concept of developing an ISP based on the flow of information from a planning stage is mentioned in many articles but has not been researched to a larger extent (Cram *et al.*, 2017; Paananen *et al.*, 2020; Rostami *et al.*, 2020). Cram *et al.* (2017) continue arguing for the lack of research of inputs within ISP development in general, but also the influence of inputs when developing an ISP at an organisational level. The evidence above identifies a gap where the limited focus has been put on the input phase and its influential consequences.

2.2 Institutional theory

Within the institutional theory, it is emphasised that organisations exist in an institutional framework that shapes their goals and processes. This framework helps to create an understanding of how organisations constitute and what they do through the effect of the environmental impact (DiMaggio and Powell, 1983). It considers the processes by which structures become established as guidelines to gain legitimacy (Scott, 2003). Spears *et al.* (2013) applied institutional theory and capability maturity model to model assurance as organisational legitimacy achieved through process maturity of security risk management

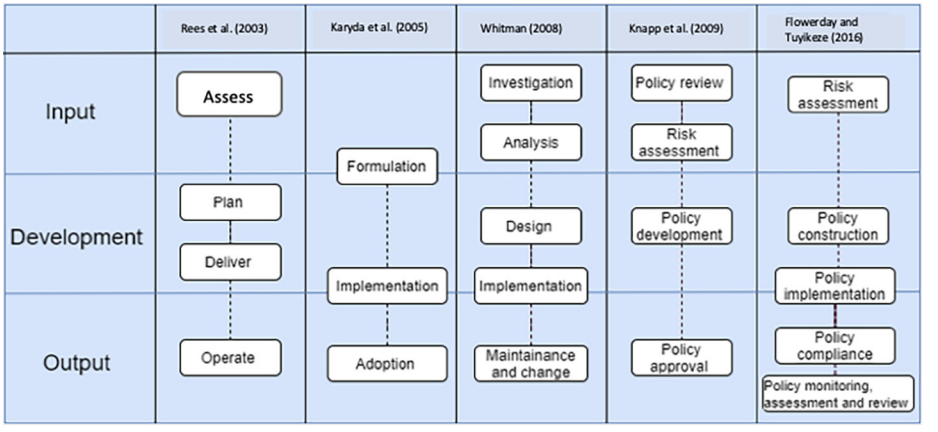

Figure 1.
Previous process models for the ISP development

practices. Furthermore, institutional theory has also been used to understand the adoption of E-government (Al-Mamari *et al.*, 2013).

2.2.1 Myths. Meyer and Rowan (1977) explain how myths create socially accepted rules, which organisations then choose to follow by creating formal structures. Myths could be processes, structures and strategies. Once these myths have become fully accepted and incorporated within an organisational field, they become institutionalised rules (Eriksson-Zetterquist, 2012).

2.2.2 Legitimacy. Legitimacy can be gained by adopting myths that organisations in the environment have already adopted (Cavusoglu *et al.*, 2015). From an institutional theory perspective, the ISP could be viewed as an answer to institutional forces pressing the organisations to conform to the prevailing ideas of what information security management should ideally be to gain legitimacy (Bjorck, 2004).

2.2.3 Isomorphism. Isomorphism, in the context of institutional theory, reflects upon the institutional pressures that power change and adoption in organisations to adopt institutional measures and requirements (DiMaggio and Powell, 1983). Furthermore, DiMaggio and Powell (1983) present the following three types of institutional pressures:

(1) *Coercive isomorphism* describes the pressures that force organisations to adopt a specific institutionalised rule-like change or practice when managing InfoSec within an organisation (Hu *et al.*, 2007).

(2) *Mimetic isomorphism* describes the pressures that refer to the submission of imitating other organisations within an organisational field to gain legitimacy (DiMaggio and Powell, 1983).

(3) *Normative isomorphism* describes the pressures that are established from the community expectation, where organisations are obligated to act as responsible member of society (DiMaggio and Powell, 1983).

2.3 Institutional theory in information security research

According to Hsu *et al.* (2012), researchers have applied different theoretical approaches to investigate critically InfoSec research. Institutional theory has been widely used and accepted across disciplines to explain whether specific organisational processes and behaviour are consistent with institutional forces (Bjorck, 2004; Cavusoglu *et al.*, 2015; Hsu, 2007). Previous studies on InfoSec through the lens of institutional theory have mainly focused on compliance and regulatory pressures (Hou *et al.*, 2018; Niemimaa and Niemimaa, 2019), where the theoretical lens mainly has been used trying to analyse the output part and results of InfoSec and connected measures.

Applying institutional theory to InfoSec research provides an opportunity to define a perspective of InfoSec as an organisational mechanism rather than a technical innovation. Studies have been done to understand the influence of internal and external institutional forces on InfoSec in organisational settings by critically reflecting upon the prescriptive and normative processes and guidelines presented in the technical paradigm in InfoSec within organisations (Hou *et al.*, 2018; Hsu *et al.*, 2012; Hu *et al.*, 2007). This study aims to understand the role of inputs in the ISP development through the lens of institutional theory.

3. A research model on inputs for information security policy development

This section aims to answer *RQ1*, to investigate what inputs are commonly used according to theory, and develop a research model to study *RQ2*.

3.1 A Literature search on inputs for information security policy development

A literature review (Webster and Watson, 2002) was conducted to answer the question of what inputs should be used when developing an ISP. This literature review investigated what current research highlights as relevant inputs and analyse what inputs are most prominent. We searched for literature through the Web of Science database since Web of Science provides comprehensive, in-depth coverage of peer-reviewed articles with high-quality content (Falagas *et al.*, 2008) and covers over 12,000 the high-impact journals and more than 150,000 conference proceedings (Franke and Brynielsson, 2014). We used a wide set of search strings for this study. The used search strings are as follows: ((“information security polic*” OR “Cyber Security Polic*"OR"information systems security polic*”) AND (Develop* OR Design OR implement* OR Formulat*)). Papers published in the database between 1975 and 2020 were included in our study. The year 1975 was selected because Web of Science databased covers publications from 1975. The literature search included journal papers, conference papers and workshop papers regardless of the geographic region to have an inclusive view of the existing research. The used search fields included the article title, abstract and keywords.

Firstly, the search with predefined search strings in Web of Science database resulted in a data set of 299 articles. Secondly, we applied our inclusion criteria presented in Table 1. This was done by reading the titles and abstracts of the potential papers by two of the authors. As a result, a total of 18 relevant articles (Appendix 1) were identified. These papers were used as the data set to identify inputs for ISP development.

Content analysis was carried out to identify inputs for ISP development from the data set. Firstly, two authors separately read and analysed these 18 articles to identify inputs for ISP development. The six inputs from (Karyda *et al.*, 2005) were used as the starting point to identify inputs from the collected articles. If any input in addition to these six inputs has been identified in the other papers, this input was recorded as additional input from the analysis. Secondly, the two authors also separately counted the number of articles mentioning each specific input. Thirdly, two authors had a discussion to synthesise their analysis results. Disagreements between the two authors and unclear aspects of the reviewed papers were discussed and resolved in this discussion. As a result, ten inputs for ISP development have been identified. The inputs are sorted according to the number of times they are mentioned. Table 2 illustrates the definition of the identified inputs, cited exemplar papers on each input and the number of articles mentioning each input.

3.2 Selected inputs for the research model

In this research, we focused on some key inputs identified from the literature review to proceed with the study on *RQ2*. The results from *RQ1* provided the ground to develop a research model to study *RQ2* to compare theory with practice. The following criteria have

Table 1.
Inclusion criteria

No.	Inclusion criteria
1.	The article is written in English.
2.	The content of the article applicable to answer *RQ1*

Input	Definition	No. of articles mentioning a specific input	Example paper(s) Cited
Risk assessment	A risk assessment recognises the business assets that an organisation wants to protect and identifies the potential threats the organisation pose connected to those assets.	14	(Karyda *et al.*, 2005) (Knapp *et al.*, 2009)
Industry standards and guidelines	Industry standards and guidelines, from a general perspective, are meant to provide uniformity that would ease an understanding and management of a concerned area.	14	(Karyda *et al.*, 2005) (Knapp *et al.*, 2009)
Regulations	Regulations can be seen as necessary measures for the organisation to comply with regulatory and legal requirements which may affect them.	13	(Karyda *et al.*, 2005) (Knapp *et al.*, 2009)
Existing Policies within the organisation	Existing Policies are the policies have been used in the organisation previously.	9	(Karyda *et al.*, 2005) (Knapp *et al.*, 2009)
State of the organisation	It refers to the information on the structure and cultural characteristics of the organisation.	5	(Karyda *et al.*, 2005)
Business requirements	It refers to requirements and objectives from the business.	4	(Paananen *et al.*, 2020)
Customer requirements	It refers to requirements from customers.	3	(Flowerday and Tuyikeze, 2016)
Desired structure and format	It refers to the aims and objectives of an organisation's security policies, in terms of length, clarity and level of detail.	3	(Cram *et al.*, 2017)
IT controls/security controls knowledge	It refers to the knowledge on IT controls/security controls.	2	(Karyda *et al.*, 2005)
Contractual Obligation	It refers to something which is required to do because of a binding contract.	1	(Paananen *et al.*, 2020)

Table 2.
Identified inputs

been applied to select the key inputs to develop the research model. The inputs included in the research model should have been mentioned in at least 50% of the papers used in the review. As the number of papers was in total 18, a single input had to be mentioned in at least nine of them. After applying these criteria, the following four prominent inputs were selected to develop the research model, to analyse how they influence the ISP development process.

3.2.1 Risk assessment. A risk assessment recognises the business assets that an organisation wants to protect and identifies the potential threats the organisation pose connected to those assets (Rees *et al.*, 2003). Previous literature states the importance of making a risk assessment before conducting the development of an ISP (Doherty *et al.*, 2009; Knapp *et al.*, 2009). Therefore, organisations must determine how important and vulnerable their information assets are and what risk they face.

3.2.2 Industry Standards and guidelines. Industry standards and guidelines, from a general perspective, are meant to provide uniformity that would ease an understanding and management of a concerned area. For instance, industry standards can offer recommendations and best practices to help organisations establish InfoSec within the organisation, of which ISP serves as a dominant aspect (Knapp *et al.*, 2009; Whitman, 2008). Using a standard as an input to influence the ISP development both helps establish a common baseline within the organisation and also creates an acceptance as adequate by external actors (Bayuk, 2009).

3.2.3 Regulations. Even if an ISP is not forced by law to exist in an organisation, the ISP could function as a framework for how to comply with existing regulations (Spears, 2007). Regulations, legislation and other constitutions act as a potent instrument in society and play a vital role in building InfoSec both nationally and internationally. Kissoon (2020) found that compliance with regulation was an important factor used by the government when investing in cybersecurity controls. Together with the increase in regulations regarding privacy and InfoSec, growing pressure to comply with regulations has become more important (Niemimaa and Niemimaa, 2019). An ISP should include necessary measures for the organisation to comply with regulatory and legal requirements which may affect them (Tuyikeze and Pottas, 2011).

3.2.4 Existing policies within the organisation. Existing policies within the organisation are another key input identified from the literature review. According to Maynard (2010), when developing an ISP, similar policies could be helpful in giving some ideas on like what an ISP should look. According to the literature review, previous studies mainly state the importance of reviewing existing policies as input but lack to describe how this should be done.

As a result, a research model has been developed (Figure 2) to analyse the actual influence of the identified inputs in practice. The inputs presented in the model are established from the findings of the literature review (i.e. Table 2). In addition, the proposed way of using these inputs for ISP development has been incorporated into Figure 2. The model will be used as a foundation for developing interview questions to investigate *RQ2* and to compare theory and practice in developing an ISP.

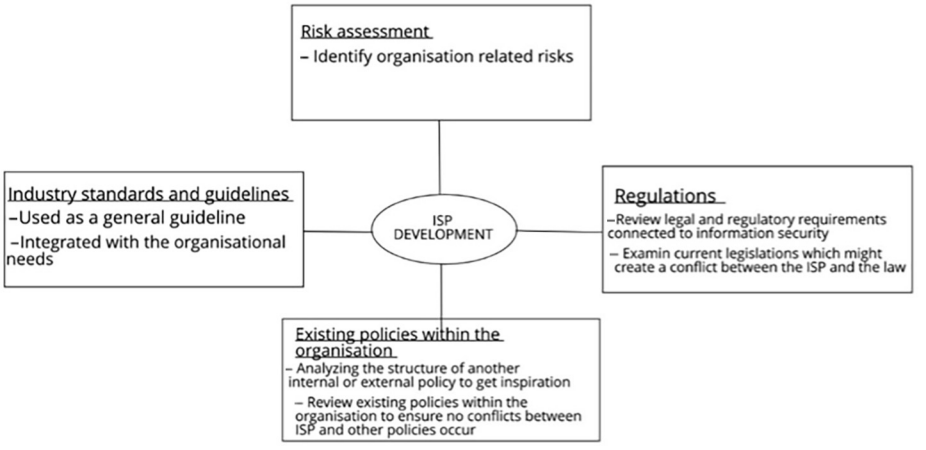

Figure 2.
Research model

4. A Study on the influence of inputs on the information security policy development process in practice

This study followed an interpretive perspective. An interpretive approach through the lens of institutional theory is applied to investigate the role of inputs in ISP development.

4.1 Formulation of interview questions

The interview questions (Appendix 2) were based on the inputs in the developed research model (i.e. Figure 2). The interview questions were developed on the following two principles: reflecting a good understanding of what previous literature is stating and arguing for each input and providing an opportunity to compare theory to practice. For instance, to study how to use risk assessments in ISP development in practice, interview questions such as:

Q1. What role does risk assessment play when developing the ISP?

Q2. How useful are the results of security recommendations from a risk assessment?

Were developed. These questions aimed to understand how the practice perceives and uses risk assessments as input. As a result, sixteen interview questions have been developed.

4.2 Selection of respondents

All interview samples were recruited from the public sector in Sweden. Qualitative data were collected from in-depth semi-structured interviews conducted with three respondents concerned with ISP development in three organisations in Sweden. They were selected based on their experience as well as their involvement and responsibility with ISP development. Table 3 presents an overview of the conducted interviews for this research. All the respondents were from Sweden. Initial contact with the respondents was made through email. The contacted respondents could, in turn, refer to other more relevant people within the field, who were then checked to see if they were suited for the study. Using the method of snowball selection made it possible to establish contact with three different people within the field of InfoSec in a short period (Bell *et al.*, 2018). Due to Covid-19 restrictions, all of the interviews were instead rescheduled to be conducted face-to-face online.

4.3 Conducting the interviews

Each interview started by describing the purpose of the interview. This approach lets the respondents understand the aims of the interview. When describing the purpose of comparing theory with practice, the respondent changed from a state of answering what they perceive is the "right answer", to answer with their own perceptions and thoughts. The developed interview questions (Appendix 2) were used for the interview. Each interview was conducted anonymously and lasted for around 45 min each. All the interviews were recorded, with consent from each respondent.

Firm	Position	Working area in public sector	Years of experience	Respondent Number
A	Head of IT Security	Active labour market policies	20 years	*R1*
B	Deputy Security Manager	Statistical services	25 years	*R2*
C	CISO	Transportation sector	10 years	*R3*

Table 3.
An overview of the respondents

4.4 Data analysis

As this research is inherently interpretivist and exploratory in nature, thematic analysis has been used for our data analysis. To present the most succinct data, the subsections on results from the interviews in Section 5 are structured as follows:

(1) if the input was being used;
(2) how it was used; and
(3) what the motivation was to use that certain input.

Three types of isomorphism from the institutional theory were applied as a theoretical lens to explain how each literature-based input influences the ISP development in practice. Furthermore, the data was also compared to what previous research presents about the use and motivation of a specific input to compare the practical use of inputs to theory.

5. Results from the interviews

This section presents and analyse the results of each input individually.

5.1 Risk assessment

None of the respondents stated that the risk assessment was used as an input to develop the ISP:

> "No special risk assessment has been done to develop the ISP." (R2)

> "I do not think it has ever been used to develop an ISP." (R3)

> "The ISP at the highest level does not need to be connected directly to a risk assessment, that is something that occurs later on." (R1).

The respondents instead describe risk-based thinking as an input when developing the ISP, where risks are informally identified and connected to the organisation and are taken into consideration. Thus, the ISP development is not directly connected to a structured risk assessment, where risks are analysed and estimated before creating the ISP.

"Underlying, the ISP is based upon some kind of risk-based thinking, but I would not say that is the main reason." (R2)

Furthermore, the risk assessment is rather connected to the underlying steering documents developed for InfoSec. The respondents describe the risk assessment as something that often is conducted after an ISP has been implemented and to investigate risks connected to the organisation:

> "I do not think that risk assessment has to play an important role in the ISP design itself, but rather what is designed afterwards." (R1)

> "The underlying documents have more of a connection to risk assessments, while the ISP is more static." (R2)

> "ISP sets the framework, before assessing the risks." (R3)

None of the respondents experienced any formal or informal requirements to conduct a risk analysis before developing an ISP. DiMaggio and Powell (1983) indicated that coercive pressure forced the organisation to act in line with certain rules and practices within IS. An alternative answer would be a reflection of seeing risk assessment as something that is not obligated to follow yet to conduct instead of perceiving risk assessment as a beneficial task (Doherty *et al.*, 2009; Knapp *et al.*, 2009; Von Solms, 1999). By not experiencing risk

assessment as an input that is established or presented from demands and expectations, it could result in not using a structured risk assessment as an input when developing an ISP.

5.1.1 The results discussion. According to this finding, none of the respondents stated that a risk assessment was conducted as an input when developing an ISP. However, the respondents emphasised the importance of having risk-based thinking when developing an ISP. This result could reflect upon an alternative way of developing an ISP, where the risks are not central in the first round of developing formal documents for InfoSec. Cram *et al.* (2017) describe risk assessment connected to the ISP development as an area that needs further research, as the current research lacks an understanding of how such input is used. A possible explanation of why the risk assessments are translated into risk-based thinking within the majority of the respondents could be described as a result of the lack of defining what a risk assessment implies. For instance, as the ISP document often is referred to as a top document to steer the organisation, it is defined as rather general and abstract.

5.2 Industry standards and guidelines

All respondents stated that industry standards and guidelines played an important role when developing an ISP:

> "I would say it plays an extremely important role. To have something that is connected and that everyone understands." (R1)

> "A standard plays a quite important role." (R2)

> "It plays a very important role. I believe almost all work is established from standards."(R3)

All respondents described the use of standards as adoption to how the organisation works and what aspects are vital to consider. By so, what parts of a standard are important to follow, is highly dependent upon how the organisation works and what is applicable.

Furthermore, all of the respondents described that they were using ISO 27001 on demands from MSB (The Swedish Civil Contingencies Agency), but also to follow a framework that is consistent and applicable regardless of the organisation. As the public sector change and communication information within different authorities, it becomes important to follow a consistent structure, depending on the organisation.

"It is extremely important to have and establish from the beginning, to create an understanding, or to create a possibility for others to understand how to think." (R1)

The above statements can be reflected upon as an answer to mimetic isomorphism (Meyer and Rowan, 1977). As organisations only are recommended by authorities to follow such a standard, the respondents are stating the importance of creating a common ground between authorities. This common ground could be reflected in organisations' mimetic pressures (DiMaggio and Powell, 1983).

One main argument for using standards was the recommendations from MSB, who refer to ISO 27001 for other authorities to use in their work with IS. The respondents all ascertain that they used ISO 27001 because MSB refers to that specific standard. However, there was no clear answer to which the recommendations were formal or informal:

> "You make it very difficult for you if you say that you will find and use something that is more suitable or better than ISO 27001." (R3)

> "The directions say that the ISP should be developed according to ISO 27000 series." (R3)

> "MSB points out that it is applicable to follow. So, there is not much choice." (R2)

The above statements can be seen as the coercive pressure stemming from higher authorities that recommend an organisation to follow the ISO 27000-series. In line with what the respondents are stating, these pressures can be experienced as forced or persuaded, according to DiMaggio and Powell (1983).

5.2.1 The results discussion. According to the respondents, industry standards and guidelines are often used as a common ground for developing an ISP. When we reflect upon the literature, Bayuk (2009) describes one of the objectives of using a standard is to help establish a common baseline, both within the organisation and outside actors. Thus, the motivation for using a standard is also established from another direction, where MSB refers to a specific standard, ISO 27000-series, that is recommended to use.

5.3 Regulations

All respondents stated that regulations played an important role when developing an ISP. The regulations are not directly connected to a requirement that states that an ISP should exist but rather play a vital role in what the ISP should contain:

> "Laws and regulations have been superior in the development." (R1)

> "Connected to the prescript written by MSB, we do not really have a choice." (R2)

> "An ISP explains that one must follow laws and regulations. Such factors affect how the policy is designed." (R3)

An ISP describes what laws and regulations to follow. Further, regulations play an even more important role in the ISP of steering documents:

> "Many of the laws and regulations are covered further down in the ISP hierarchy." (R3)

The motivation of using regulations as input is often obligated, as an organisation that is not following a law can be punished.

> "If the rules are not followed, there will be regulatory authorities or other institutions who will make a note on that." (R2)

The influence of regulations on developing an ISP reflects upon coercive pressure. According to the description of coercive pressure from DiMaggio and Powell (1983), the requirements for using such input stem from governmental laws, political influences and supervisory authorities.

However, one of the respondents was discussing that requirements of following a certain law did not always have to be based upon a forcing law but could be based upon requirements from the top management.

"Some of the laws are forced, while others are internally controlled by the CEO or the General Director, who has their own imprints." (R1)

Accordingly, the incentive of following certain regulations is established both from outside and inside an organisation.

5.3.1 The results discussion. According to the respondents, regulations differ somewhat from the other inputs as they often are obligated. If the organisation is not following the rules, it can be punished.

5.4 Existing policies within the organisation

According to the respondents, what role other policies in an organisation play when developing an ISP seem to be diffuse:

> "From knowledge about the organisation, it is rather important to include in the process. But it is not as important if the ISP needs to be re-built our re-designed." (R1)
>
> "I do not actually think it has that great of an impact." (R2)
>
> "I am not really sure if analysing other policies in the organisation would matter."(R3)

How to use existing policies as inputs are reflected in the mapping process. It depends on the analysis of what information that currently exists, and what needs to be covered.

"We are looking at the policies and then map them. We are checking like 'Do we cover everything' so that different policies work together." (R^2)

Furthermore, a reflection of other existing policies in an organisation when developing an ISP is used to anchor the ISP into the organisation. Other existing policies are to be seen as a reflection of the organisation:

> "To design an ISP without considering other policies could result in difficulties when trying to anchor the work." (R1)
>
> "You try as much as possible to reflect upon how much impact it will have in other areas of the organisation." (R2)
>
> "I do not believe there are that many conflicts between policies, however, it might not result in what is desired with the ISP, if you do not pay attention to what already exists in the organisation." (R3)

Through the lens of institutional theory, what role other existing policies play to influence the ISP development within an organisation could be explained by the influence of normative pressure. As Hsu *et al.* (2012) point out, such normative pressure on how to use input is derived from professionalisation. Furthermore, Kam *et al.* (2013) describe normative isomorphism as an adjusted behaviour based on beliefs of what is appropriate to meet expectations from stakeholders.

5.4.1 The results discussion. The question of what role other existing policies in an organisation has in the ISP development does not have a precise answer. Within some organisations, reviewing other policies seems to play an important role when developing an ISP. On the one hand, Maynard and Ruighaver (2003) describe how reviewing other policies in an organisation can help establish a common structure of how the ISP should be developed. On the other hand, Whitman (2008) describes that reviewing other policies is helpful to understand what needs to be changed in the organisation by mapping policies with each other. In line with the literature above, the respondents present the use of reviewing other policies similarly.

6. Discussion and conclusion

6.1 Theoretical contributions

This study made several contributions to the existing research on ISP development. Firstly, this research identified ten inputs for ISP development and contributed to the current literature on inputs for ISP development. Secondly, most previous studies (Niemimaa and Niemimaa, 2019) that tend to focus on the output part of ISP development and connected measures. This research contributes to an alternative perspective that complements previous studies by focusing on the use of the input part of ISP development through the lens of institutional theory. Thirdly, it has also investigated and compared theory to practice on the influence of inputs in the ISP development. A lack of studies between theory and practice has been indicated in previous studies (Cram *et al.*, 2017; Paananen *et al.*, 2020). By adopting a socio-organisational perspective into the field of ISP development process, the results generated an alternative understanding of the use of inputs in ISP development. This

study addresses the impact of the coercive, mimetic and normative pressures on the use of four inputs in practice and signifies the influence of inputs on ISP development can be derived from institutionalised rules or practices established by higher authorities.

6.2 Practical implications

Investigating the ISP development process from an institutional perspective implies the importance of reflecting upon more than rational choices by including institutional pressures and organisational contexts when using inputs in the ISP development. Based on the results, this research recommends five practical implications for practitioners working with the ISP development. These recommendations aim to create an understanding of how an ISP could be developed, considering more than the rational functionalist perspective.

- *Recommendation 1: define what an ISP means for the organisation.* An ISP could be defined differently with different purposes, depending on the organisation. Defining what purpose an ISP has in the specific organisation will facilitate the search for the right support in theory, as well as anchoring the ISP into practice.
- *Recommendation 2: understand what organisational context makes an input important.* It is essential to have a good understanding of the organisational context in which an ISP should be developed. Practitioners need to consider what inputs are affecting other processes or practices in the organisation. These inputs would most likely be affecting ISP development as well.
- *Recommendation 3: understand institutional pressures as an effect to use input.* Although input plays an important role in the ISP development, it is important to consider from where the sense of importance stems. Acknowledging the source of importance could be a useful guideline for understanding why input is being used.
- *Recommendation 4: acknowledge an ISP as a part of legitimacy, not the source of legitimacy.* Considering the ISP document act as a source of legitimacy would not help clarify what purpose an ISP ideally should fulfil, since the ISP document is not acknowledged as a part of legitimacy in the organisational context. Consequently, it would be more difficult to anchor the ISP into the organisation.
- *Recommendation 5: the overall perception of InfoSec would affect how inputs are used in the ISP development process.* The overall perception of InfoSec will affect what ought to be important in the ISP development process. Understanding this perception could facilitate the most suitable use of inputs and further development of an ISP in a specific organisation.

6.3 Key conclusions

Firstly, this research identified ten inputs for ISP development from a literature search and developed a research model consisting of the four major inputs. Secondly, this study shows that the influence of inputs on the ISP development is affected upon more than the rational functionalistic choices. We find that the influence of inputs on the ISP development can be derived from institutionalised rule-like change or practice established by higher authorities; actions and practices that are perceived as successful and often used by other organisations; or the beliefs of what is viewed as appropriate to meet the specific pressures from stakeholders.

6.4 Limitations

Like all research, this study is not without limitations. Firstly, the number of respondents in this study was quite small. Secondly, although ten inputs have been identified from the literature review, only four inputs have been included in the research model. Thus, further

study on other inputs would provide another opportunity to generate additional insight into the influences of inputs in the ISP development process. Thirdly, only one theoretical lens has been selected to analyse the results. Choosing a theoretical lens can enable a new perspective on a research subject. However, choosing the theoretical lens also implies that other theoretical lenses are excluded from the subject. Finally, all the interviewees in this study were from Sweden. The generalisability of the results to other countries needs to be further explored.

6.5 Future research directions

It also exists some opportunities for future research. Firstly, future studies can be carried out to examine the influence of the other identified inputs from the literature on ISP development. As this study limited the scope of the research to four identified inputs, the need for further understanding of the practitioners' use of other inputs is needed. Secondly, to widen the knowledge of the role of inputs in the ISP development, deep analysis with additional data from a larger number of InfoSec practitioners is encouraged. Thirdly, another study with respondents from other countries could be carried out to verify the findings from this study further.

References

Al-Mamari, Q., Corbitt, B. and Oyaro Gekara, V. (2013), "E-government adoption in Oman: motivating factors from a government perspective", *Transforming Government: People, Process and Policy*, Vol. 7 No. 2, pp. 199-224, doi: 10.1108/17506161311325369.

Bayuk, J. (2009), "How to write an information security policy", Computerworld, available at; www.computerworld.com/article/2525539/how-to-write-an-information-security-policy.html

Bell, E., Bryman, A. and Harley, B. (2018), Business Research Methods, Oxford University Press, United Kingdom.

Bjorck, F. (2004), "Institutional theory: a new perspective for research into is/IT security in organisations", Paper presented at the Proceedings of the 37th Annual HI International Conference on System Sciences, 2004, Big Island, HI.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y. and Benbasat, I. (2015), "Institutional pressures in security management: direct and indirect influences on organizational investment in information security control resources", *Information and Management*, Vol. 52 No. 4, pp. 385-400.

Chen, Y., Galletta, D.F., Lowry, P.B., Luo, X., Moody, G.D. and Willison, R. (2021), "Understanding inconsistent employee compliance with information security policies through the lens of the extended parallel process model", *Information Systems Research*, Vol. 32 No. 3, pp. 1043-1065.

Cram, W.A., Proudfoot, J.G. and D'arcy, J. (2017), "Organizational information security policies: a review and research framework", *European Journal of Information Systems*, Vol. 26 No. 6, pp. 605-641.

DiMaggio, P.J. and Powell, W.W. (1983), "The iron cage revisited: institutional isomorphism and collective rationality in organizational fields", *American Sociological Review*, Vol. 48 No. 2, pp. 147-160.

Doherty, N.F., Anastasakis, L. and Fulford, H. (2009), "The information security policy unpacked: a critical study of the content of university policies", *International Journal of Information Management*, Vol. 29 No. 6, pp. 449-457.

Ellefsen, I. (2014), "The development of a cyber security policy in developing regions and the impact on stakeholders", Paper presented at the 2014 Ist-Africa Conference Proceedings, MAURITIUS.

Eriksson-Zetterquist, U. (2012), Institutionell Teori:-Idéer, Moden, Förändring, Liber AB, Stockholm, Sweden.

Falagas, M.E., Pitsouni, E.I., Malietzis, G.-A. and Pappas, G. (2008), "Comparison of pubMed, scopus, web of science, and google scholar: strengths and weaknesses", *The FASEB journal*, Vol. 22 No. 2, pp. 338-342.

Flowerday, S.V. and Tuyikeze, T. (2016), "Information security policy development and implementation: the what, how and who", *Computers and Security*, Vol. 61, pp. 169-183, doi: 10.1016/j.cose.2016.06.002.

Franke, U. and Brynielsson, J. (2014), "Cyber situational awareness – a systematic review of the literature", *Computers and Security*, Vol. 46, pp. 18-31.

Goel, S. and Chengalur-Smith, I.N. (2010), "Metrics for characterizing the form of security policies", *The Journal of Strategic Information Systems*, Vol. 19 No. 4, pp. 281-295.

Höne, K. and Eloff, J.H.P. (2002), "Information security policy – what do international information security standards say?", *Computers and Security*, Vol. 21 No. 5, pp. 402-409.

Hou, Y., Gao, P. and Nicholson, B. (2018), "Understanding organisational responses to regulative pressures in information security management: the case of a chinese hospital", *Technological Forecasting and Social Change*, Vol. 126, pp. 64-75.

Hsu, C. (2007), "Making sense of institutionalizing information systems security management in organizations", Paper presented at the International Conference on Information Systems (ICIS 2007), Montreal.

Hsu, C., Lee, J.-N. and Straub, D.W. (2012), "Institutional influences on information systems security innovations", *Information Systems Research*, Vol. 23 No. 3-part-2, pp. 918-939.

Hu, Q., Hart, P. and Cooke, D. (2007), "The role of external and internal influences on information systems security – a neo-institutional perspective", *The Journal of Strategic Information Systems*, Vol. 16 No. 2, pp. 153-172.

Ismail, W.B.W., Widyarto, S., Ahmad, R.A.T.R. and A. and Ghani, K. (2017), "A generic framework for information security policy development", Paper presented at the 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI).

Kam, H.J., Katerattanakul, P., Gogolin, G. and Hong, S. (2013), "Information security policy compliance in higher education: a neo-institutional perspective", Paper presented at the 17th Pacific Asia Conference on Information Systems, PACIS 2013, Jeju Island.

Karyda, M., Kiountouzis, E. and Kokolakis, S. (2005), "Information systems security policies: a contextual perspective", *Computers and Security*, Vol. 24 No. 3, pp. 246-260.

Khando, K., Gao, S., Islam, S.M. and Salman, A. (2021), "Enhancing employees information security awareness in private and public organisations: a systematic literature review", *Computers and Security*, Vol. 106, p. 102267, doi: 10.1016/j.cose.2021.102267.

Kinnunen, H. (2017), "Critical considerations for organisation-specific information security policy development", Paper presented at the International Conference on Transformations and Innovations in Management (ICTIM 2017), Shanghai.

Kissoon, T. (2020), "Optimum spending on cyber security measures", *Transforming Government: People, Process and Policy*, Vol. 14 No. 3, pp. 417-431, doi: 10.1108/TG-11-2019-0112.

Knapp, K.J., Morris, R.F. Jr, Marshall, T.E. and Byrd, T.A. (2009), "Information security policy: an organizational-level process model", *Computers and Security*, Vol. 28 No. 7, pp. 493-508.

Ku, C.Y., Chang, Y.W. and Yen, D.C. (2009), "National information security policy and its implementation: a case study in Taiwan", *Telecommunications Policy*, Vol. 33 No. 7, pp. 371-384.

Lopes, I. and Oliveira, P. (2015), "Applying action research in the formulation of information security policies", *New Contributions in Information Systems and Technologies*, Springer, Berlin/ Heidelberg, Germany, pp. 513-522.

Maynard, S. (2010), *Strategic Information Security Policy Quality Assessment: A Multiple Constituency Perspective*, University of Melbourne, Melbourne, Australia.

Maynard, S. and Ruighaver, A. (2003), "Development and evaluation of information system security policies", in Hunter, M.G. and Dhanda, K.K. (Eds), *Information Systems: The Challenges of Theory and Practice, The Information Institute*, Las Vegas, NV.

Meyer, J.W. and Rowan, B. (1977), "Institutionalized organizations: formal structure as myth and ceremony", *American Journal of Sociology*, Vol. 83 No. 2, pp. 340-363.

Niemimaa, M. and Niemimaa, E. (2019), "Abductive innovations in information security policy development: an ethnographic study", *European Journal of Information Systems*, Vol. 28 No. 5, pp. 566-589.

Paananen, H., Lake, M. and Siponen, M. (2020), "State of the art in information security policy development", *Computers and Security*, Vol. 88, p. 101608, doi: 10.1016/j.cose.2019.101608.

Rees, J., Bandyopadhyay, S. and Spafford, E.H. (2003), "PFIRES: a policy framework for information security", *Communications of the ACM*, Vol. 46 No. 7, pp. 101-106.

Rostami, E., Karlsson, F. and Kolkowska, E. (2020), "The hunt for computerized support in information security policy management: a literature review", *Information and Computer Security*, Vol. 28 No. 2, pp. 215-259.

Scott, R. (2003), *Organizations. Rational, Natural, and Open Systems*, Prentice Hall, NJ.

Simms, D.J. (2009), "Information security optimization: from theory to practice", Paper presented at the 2009 International Conference on Availability, Reliability and Security.

Spears, J. (2007), "Institutionalizing information security risk management: a multi-method empirical study on the effects of regulation", (PhD). The Pennsylvania State University.

Spears, J., Barki, H. and Barton, R.R. (2013), "Theorizing the concept and role of assurance in information systems security", *Information and Management*, Vol. 50 No. 7, pp. 598-605, doi: 10.1016/j.im.2013.08.004.

Stitilis, D., Pakutinskas, P. and Malinauskaite, I. (2016), "Preconditions of sustainable ecosystem: cyber security policy and strategies", *Entrepreneurship and Sustainability Issues*, Vol. 4 No. 2, pp. 174-182, doi: 10.9770/jesi.2016.4.2(5).

Tagarev, T. and Polimirova, D. (2019), "Main considerations in elaborating organizational information security policies", Paper presented at the Proceedings of the 20th International Conference on Computer Systems and Technologies, Ruse, doi; 10.1145/3345252.3345302.

Tuyikeze, T. and Pottas, D. (2011), "An information security policy development life cycle", Paper presented at the Proceedings of the South African Information Security Multi-Conference (SAISMC), Port Elizabeth.

Von Solms, R. (1999), "Information security management: why standards are important", *Information Management and Computer Security*, Vol. 7 No. 1, pp. 50-58.

Webster, J. and Watson, R.T. (2002), "Analyzing the past to prepare for the future: writing a literature review", *Management Information Systems Quarterly*, Vol. 26 No. 2, p. 3.

Whitman, M.E. (2008), "Security policy: from design to maintenance", in Straub, D.W., Goodman, S. and Baskerville, R.L. (Eds), *Information Security: Policy, Processes, and Practices*, M.E. Sharpe, Armonk, NY, pp. 123-151.

Yang, T.-H., Ku, C.-Y. and Liu, M.-N. (2016), "An integrated system for information security management with the unified framework", *Journal of Risk Research*, Vol. 19 No. 1, pp. 21-41.

Appendix 1. the list of the 18 reviewed articles

Reviewed 18 articles	(Paananen *et al.*, 2020) (Niemimaa and Niemimaa, 2019) (Tagarev and Polimirova, 2019) (Cram *et al.*, 2017) (Kinnunen, 2017) (Ismail *et al.*, 2017) (Stitilis *et al.*, 2016; Flowerday and Tuyikeze, 2016; Lopes and Oliveira, 2015; Ellefsen, 2014; Tuyikeze and Pottas, 2011) (Knapp *et al.*, 2009; Ku, Chang, and Yen, 2009; Simms, 2009; Yang, Ku, and Liu, 2016; Karyda *et al.*, 2005; Doherty *et al.*, 2009; Höne and Eloff, 2002)

Appendix 2. Interview questions

Input 1: risk assessment

What role does risk assessment play when developing the ISP?

What are your thoughts on risk assessments? Are they important?

Are there pressures to do a risk assessment before designing an ISP? If so, from where and how?

Would it be possible to design a sufficient ISP without risk assessment as an input?

Input 2: industry standards and guidelines

What role do industry standards and guidelines play when developing the ISP?

What are your thoughts of industry standards and guidelines, are they important?

Are there pressures to use industry standards or guidelines? If so, from where and how?

Would it be possible to design a sufficient ISP without industry standards and guidelines as an input?

Input 3: regulations

What role do regulations play when developing the ISP?

What are your thoughts of regulations, are they important?

Are there pressures to follow regulations? If so, from where and how?

Would it be possible to design a sufficient ISP without considering regulations as an input?

Input 4: existing policies within the organisation

What role do existing policies within the organisation play when developing the ISP?

What are your thoughts of existing policies within the organisation, are they important?

Are there pressures to consider existing policies within the organisation? If so, from where and how?

Would it be possible to design a sufficient ISP without considering existing policies within the organisation as an input?

About the authors

Lovisa Göransson Ording obtained her MSc in Information Security Management in 2020 from Örebro University, Sweden. Her research interest includes information security policy development, and information security management.

Dr Shang Gao is an Associate Professor in Information Systems at Örebro University, Sweden. He obtained his PhD in Information Systems in 2011 from the Norwegian University of Science and Technology, Norway. His research interests include mobile information systems, technology diffusion, information security management, information systems modelling and requirement engineering. He has published more than 80 refereed papers in journals, books and archival proceedings since 2006. Shang Gao is the corresponding author and can be contacted at: shang.gao@oru.se

Dr Weifeng Chen is an Associate Professor at Brunel University Business School London (UK) specialising in international business strategy, international innovation management, brand management and Chinese Brands. His research has been published in *Regional Studies*, the *Journal of Organisational Change Management*, the *International Journal of Production Economics*, *European Journal of Marketing*, the *Journal of Information System Management* and the *Journal of Business Research*.