Policy components – a conceptual model for modularizing and tailoring of information security policies

Elham Rostami, Fredrik Karlsson and Shang Gao
Department of Informatics, Örebro University, Örebro, Sweden

Received 11 October 2022
Revised 9 December 2022
Accepted 9 December 2022

Abstract

Purpose – This paper aims to propose a conceptual model of policy components for software that supports modularizing and tailoring of information security policies (ISPs).

Design/methodology/approach – This study used a design science research approach, drawing on design knowledge from the field of situational method engineering. The conceptual model was developed as a unified modeling language class diagram using existing ISPs from public agencies in Sweden.

Findings – This study's demonstration as proof of concept indicates that the conceptual model can be used to create free-standing modules that provide guidance about information security in relation to a specific work task and that these modules can be used across multiple tailored ISPs. Thus, the model can be considered as a step toward developing software to tailor ISPs.

Research limitations/implications – The proposed conceptual model bears several short- and long-term implications for research. In the short term, the model can act as a foundation for developing software to design tailored ISPs. In the long term, having software that enables tailorable ISPs will allow researchers to do new types of studies, such as evaluating the software's effectiveness in the ISP development process.

Practical implications – Practitioners can use the model to develop software that assist information security managers in designing tailored ISPs. Such a tool can offer the opportunity for information security managers to design more purposeful ISPs.

Originality/value – The proposed model offers a detailed and well-elaborated starting point for developing software that supports modularizing and tailoring of ISPs.

Keywords Information security policy, Information security management, Policy component, Situational method engineering, Policy design

Paper type Research paper

1. Introduction

In contemporary organizations many business processes are highly dependent on information assets. Therefore, information security, where the purpose is to safeguard an organization's information assets, is critical. Organizations can choose to implement controls, i.e. measures that address risks, to enhance information security. These controls are often sorted into three main categories:

Information & Computer Security
Vol. 31 No. 3, 2023
pp. 331-352
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-10-2022-0160

(1) technical;
(2) formal; and
(3) informal controls (Dhillon, 2017).

Technical controls are for example antivirus, antispyware and firewalls. Still, protecting information assets is not only a technical issue (Sheng *et al.*, 2010). Among the formal controls, information security policy (ISP), is viewed as one of the most important ones. An ISP includes "established rules that provide guidance in the protection of an organization's assets" (Whitman, 2008) and directs employees' use of information and information systems, i.e. information assets. Finally, informal controls address social aspects, such as enhancing employees' awareness of information security issues through education and training programs.

At the same time, employees' noncompliance with ISPs has been acknowledged as a perennial problem in practice (Ernst and Young, 2008; Ernst and Young, 2010; PwC, 2014; PwC, 2018). Researchers have explored both individual-related factors that explain these behaviors (Herath and Rao, 2009; Nash and Greenwood, 2008; Siponen *et al.*, 2014; Stanton *et al.*, 2005) and how security education, training and awareness programs can address this problem (Kruger and Kearney, 2006; Albrechtsen and Hovden, 2010; Puhakainen and Siponen, 2010; Abraham and Chengalur-Smith, 2019). At the same time, half of all information security breaches caused by employees are accidental (ENISA, 2014). It has therefore been argued that there is also an ISP-design related aspect to employees' noncompliance (Karlsson *et al.*, 2017), where ISPs can be cumbersome to follow, contradictory and sometimes even incompatible with existing work practice (Adams and Sasse, 1999; Stahl *et al.*, 2012). Of course, over the years, researchers have suggested different types of ISP design support that provide advice to practitioners (Gritzalis, 1997; Ismail and Widyarto, 2016; Lindup, 1995; Lopes and Oliveira, 2015; Siponen and Iivari, 2006; Renaud and Goucher, 2012). In addition, there are different practitioner guidelines and standards (i.e. ISO 27000 series) that support this work.

However, as has been shown by Rostami (2019), existing research mostly takes a monolithic view of ISPs, where the same ISP is used for the entire organization, i.e. for all employees. Thus, there is a relevance issue with ISPs. Having said that, some researchers have acknowledged that the needs of employees differ (Wood, 1995; Baskerville and Siponen, 2002; Cosic and Boban, 2010; Höne and Eloff, 2002a; Palmer *et al.*, 2001; Karlsson *et al.*, 2017; Simms, 2009), which means that not all parts of an ISP are equally relevant for all employees. Thus, this suggests pursuing a tailoring approach to ISPs.

Furthermore, designing ISPs is a nontrivial task (Kinnunen and Siponen, 2018), which means there is a design burden on information security managers. Researchers have therefore suggested software to aid the management of ISPs (Vermeulen and Von Solms, 2002; Coertze *et al.*, 2011; Coertze and von Solms, 2013; Syamsuddin and Hwang, 2010). For example, Vermeulen and Von Solms (2002) suggested an information system security management toolbox for developing ISPs. Notwithstanding the merits of this research, they seem to have addressed the tailoring aspect of ISPs to a very limited extent. Furthermore, these papers have focused on presenting the tools themselves, that is, illustrating the provided functionality. It means that they are limited in their contribution to design knowledge (Drechsler and Hevner, 2018) that can be used by researchers or practitioners when designing similar software. One notable exception is Rostami *et al.* (2020a), who identified two requirements about tailoring of ISPs among a larger set of requirements for software to aid ISP design.

Consequently, combining the ideas of tailoring ISPs and software to support this task could address both the relevance issue of ISPs and ease the design burden of information security managers. To facilitate consistent and coherent tailoring with the use of such software, an ISP needs to be possible to represent as modules that can be selected depending on the relevance for the audience. Therefore, this paper aims to propose a conceptual model of policy components for software that supports modularizing and tailoring of ISPs. To this end, we employed design science research (DSR) (Hevner *et al.*, 2004), and we draw on design characteristics from situational method engineering (SME). The SME discipline has a long tradition of modularizing and tailoring software development methods (Henderson-Sellers *et al.*, 2014), i.e. guiding ways of working with software development, which share similarities with guiding employees' use of information assets. It should be noted that in this paper our use of the tailoring concept includes all SME approaches, although (method) tailoring sometimes refers to a subcategory of these approaches (Henderson-Sellers *et al.*, 2014). We do so because we believe it is more important to align with how the tailoring concept has been used previously in ISP research, referring to any approach to adapt the ISP content to different target groups (Rostami *et al.*, 2020a).

The remaining part of the paper is structured as follows. Section 2 discusses existing research on software to aid the management of ISPs. Section 3 provides an overview of modularizing concepts and SME approaches to identify design characteristics that we can build on. Section 4 presents the research design. In Section 5, we present the developed conceptual model. In Section 6, the demonstration and evaluation of the model are presented. Finally, in Section 7, we discuss the findings concerning the model; this section ends with presenting the limitations and future work.

2. Related research

The use of software to aid the design of ISPs is not new in research (Hoppe *et al.*, 2002; Vermeulen and Von Solms, 2002). Simultaneously, Rostami *et al.* (2020b) found that research on this type of software has received limited attention from researchers. Instead, most research on designing ISPs has been about manual support. The few papers that have addressed computerized tools (Syamsuddin and Hwang, 2010; Coertze *et al.*, 2011; Coertze and von Solms, 2013) have focused on the software itself, i.e. demonstrating the tools' functionality and not the design knowledge used to build the software. Thus, there is a research gap regarding the conceptual models behind these tools, which can help design similar tools.

Syamsuddin and Hwang (2010) introduced a framework that helps managers when "evaluating information security policy performance." Their proposed framework, which was demonstrated as an Open Office Calc application, adopts the analytic hierarchy process to structure and understand performance. Their choice of the demonstrator was based on their goal to show that this kind of support can be provided without the use of proprietary analytic hierarchy process software. However, they did not provide design support for modularizing of ISPs.

Coertze *et al.* (2011) elaborated on the information security management toolbox that was introduced by Hoppe *et al.* (2002). They found that the existing toolbox had some limitations for small, medium and micro enterprises (SMMEs). These types of enterprises often lack the resources of larger organizations and Coertze *et al.* (2011) provided a recommendation on how the toolbox can be improved to support SMMEs. The suggested improvements for future implementation were:

- The toolbox should be cost-effective and user-centric.

- It should be Web based instead of Windows based.
- It should cover compliance and evaluation of ISPs, and it should be part of a larger information security Web portal.

All these suggestions focus on improving the functionality; however, they did not provide any conceptual model to aid this development.

Coertze and von Solms (2013) presented the information security governance toolbox, which yet again extends the work presented by Hoppe *et al.* (2002). The tool is built on the information security governance model (Coertze and von Solms, 2012), which is a process-oriented model. The software consists of two phases, a direct phase and a control phase, where the design of ISPs is part of the former phase. The direct phase also supports the selection of information security controls based on the ISP. They claim that the tool enables a dynamic ISP, where supporting information security procedures "are presented for selection based on the security controls selected." As a result, the software can draft information security documentation dynamically. The software has query-based requirements analysis and a wizard that guides the selection of information security controls and procedures. These controls and procedures originate from ISO 27002. As a result, the software drafts the ISP. Coertze and von Solms (2013) argued that the software provides a "personalized and tailormade Word-document." However, it is unclear to what extent it is tailored to the employee's work situation. Moreover, they do not provide any conceptual model to aid the implementation of such tailoring functionality.

Rostami *et al.* (2020a) identified 14 requirements for software to aid ISP design. Among these requirements two of them directly focus on tailoring ISPs: support a tailorable design of ISPs and address clear and uniform target groups. The remaining software requirements to aid ISP design are actionable advice, based on identified risks, clarifying responsibilities, clear communicative objectives, clear structure, clearly defined concepts, informed by laws, regulations and standards, internally congruent ISP actions, keep up-to-date, goal alignment and styling. Although these requirements are valuable prerequisites for developing software to support tailoring ISP, they have not turned into software or a conceptual model that can be used to implement such software.

Moving beyond the research on software that aids the design of ISPs, existing research provides some models/frameworks that support ISP design (Ismail and Widyarto, 2016; Tuyikeze and Flowerday, 2014; Flowerday and Tuyikeze, 2016). However, these models are not conceptual models, i.e. models that are representations of software. Instead, these are more process-oriented models providing step-by-step guidelines for information security managers on how to design ISPs. For example, Ismail and Widyarto (2016) proposed a model of the ISP development process. Their model consisted of three phases:

(1) the pre-development phase;
(2) the development phase; and
(3) the implementation phase.

For the development phase, they provided instructions how the ISP should be written, what kind of words should be used (i.e. use "must" instead of "never") and the importance of readability.

Another example is the ISP development model put forth by Tuyikeze and Flowerday (2014) and Flowerday and Tuyikeze (2016), which has ten components that organizations should consider in developing and implementing ISPs. The model contains five process components and five components that act as input or drivers. Although these models can

help information security managers design ISPs, they do not provide design knowledge on how to implement software that facilitates a tailoring approach to ISPs.

3. Situational method engineering

As said in the Introduction, we borrow design characteristics from the field of SME and how they create situational software development methods, to guide our DSR work with the conceptual model. Software development methods are used in the software industry to guide software developers when executing software development tasks. In other words, software development methods serve a similar purpose as ISPs, i.e. to guide actors. Software development methods are often understood to include three parts (Karlsson and Ågerfalk, 2004). First, there is a process description that informs software developers of activities that should be carried out. Second, these methods include concepts to describe the problem domain and the method itself. Finally, there is some sort of notation on how to document the results. The two first parts share similarities with ISPs, i.e. providing guidance on what to do (or not to do) and concepts that describe the information security domain or the ISP itself.

Among researchers on software development methods, there seems to be commonly agreed that there is no such thing as a one-size-fits-all software development method (Karlsson, 2013) and there has been a need to tailor these methods to the situation at hand. SME is about "creating, using and adapting a software development method based on local conditions" (Henderson-Sellers *et al.*, 2014). Thus, given that SME researchers have suggested and investigated different ways of tailoring artifacts that share a similar purpose as ISPs, it seems reasonable to draw on this research as a starting point for a tailoring approach to ISPs.

SME researchers have suggested different approaches to tailoring (Bajec *et al.*, 2007; Harmsen, 1997; Cervera, 2015; Karlsson and Ågerfalk, 2009; Ralyté and Rolland, 2001; Ralyté and Franch, 2018; Sandkuhl and Seigerroth, 2019). Although there are differences between these approaches, "they share some fundamental ideas. One of the central ideas is the method part, a small part of an existing method or method-to-be" (Goldkuhl and Karlsson, 2020). These method parts or modules are used to construct, extend or reduce a software development method. A collection of method parts is called a method base, and it is often stored in a repository, such as a database. SME implies the use of a standardized format, such as a method fragment (Harmsen *et al.*, 1994), method chunk (Rolland and Prakash, 1996) or method component (Karlsson and Wistrand, 2006). These standardized formats are needed to make the method parts reusable across multiple situational software development methods; they guarantee that a specific method part has the same content each time it is included in a situational method. Furthermore, the standardized format makes the method parts share the same internal structure, which guides how information about software development methods is modeled. It means that the standardized formats provide support to achieve internally consistent and coherent method parts, i.e. parts "without lose ends" (Wistrand and Karlsson, 2004) and that are perceived as meaningful.

One difference that exists between the standardized formats to create method parts is their granularity and the type of content they include. For example, the method fragment is a multilayered format, where the size of a fragment can range from a concept to an entire software development method (Harmsen, 1997). The more recent method component format (Karlsson and Wistrand, 2006) stresses the importance of the method parts being self-contained, i.e. that they contain enough information to provide guidance to the method part user to produce a result. It means that a method component focuses "the guidelines that describe the deliverable and the process of producing such a deliverable"

(Wistrand and Karlsson, 2004), which in information security could be interpreted as the secure use of an information asset and the steps to do so.

As said above SME offers different approaches to tailoring, such as assembly based (Ralyté and Rolland, 2001) and method configuration (Karlsson and Ågerfalk, 2009). They differ in how method parts are selected with the purpose of creating, extending and/or reducing a software development method to a situational version. Basically, an assembly-based strategy builds a situational method from scratch using selected method parts. The method configuration strategy works in the opposite direction, starting with an entire software development method which is tailored, for example, by removing method parts. Regardless of strategy, the selection of method parts to produce a situational method is made using a selection mechanism. The different approaches employ selection mechanisms of different complexities. These selection mechanisms are often based on a combination of different project requirements, such as project size, project complexity and being business critical or not (Harmsen, 1997). The project requirements are then matched with how the method parts have been classified, such as a method part that is suitable for complex projects. Thus, the method parts have attributes that contain the classification. The selection provides a set of method parts from the repository that are then used to tailor the software development method by following the steps in the SME approach. In Table 1, we summarize the characteristics of tailoring that we borrow from kernel theories in SME.

4. Research design

This research is part of a larger DSR endeavor, where the end goal is to suggest a software for tailoring of ISPs. DSR aims to introduce innovative artifacts to a problem domain and at the same time contribute with design knowledge to the existing knowledge base (Hevner *et al.*, 2004). Thus, this type of research explicitly recognizes artifacts, such as software, as research deliverables. Conceptual models, such as the one proposed in this paper, are important metaartifacts that result from the design process and have the ability to inform future designs in the problem domain (Drechsler and Hevner, 2018). This research follows the DSR approach suggested by Peffers *et al.* (2007), which includes six phases (Figure 1).

The problem identification and motivation for this study are found in the Introduction. Previous empirical studies have shown that there exists an ISP-design-related aspect to employees' noncompliance with ISPs. Existing research has suggested a tailoring approach to ISP, which we combine with the idea of software to aid information security managers with tailoring. Furthermore, in the Introduction, we defined the objective of our study, i.e. to

Characteristics	Meaning
Self-contained modules	Self-contained means that each module contains enough information to provide meaningful guidance to the module user, i.e. the employee
Internally consistent and coherent modules	All modules should share the same internal structure, guiding how module content is structured. This allows modules to be constructed without lose ends and thus its content "will be perceivable as meaningful" (Wistrand and Karlsson, 2004)
Reusable modules	The modules should be free-standing and possible to reuse across multiple tailored artefacts, i.e. the modules should be possible to reuse reusable across multiple ISPs
Selection mechanism	Relevant modules should be selected using a selection mechanism that is relevant for the situation at hand, i.e. why one tailored ISP differ from another tailored ISP

Table 1.
Characteristic borrowed from kernel theories in situational method engineering

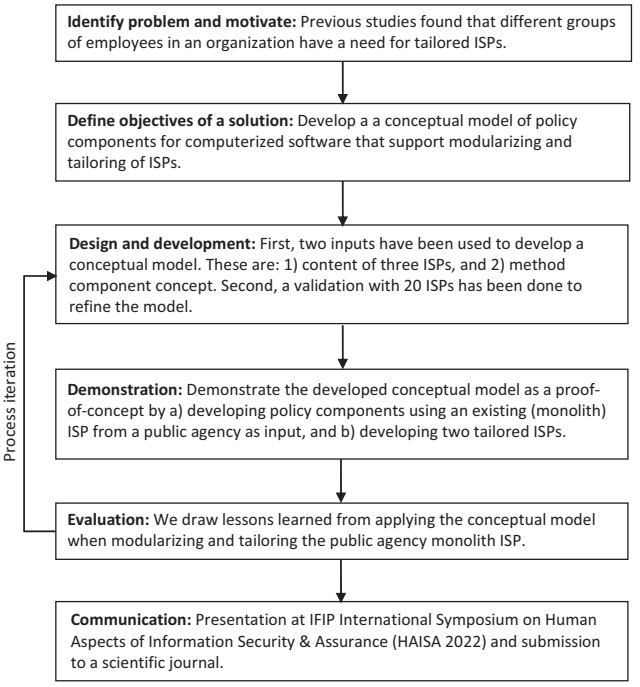

Figure 1.
Nominal design science phase model adapted from Peffers *et al.* (2007)

propose a conceptual model of policy components for software that support modularizing and tailoring of ISPs. This objective was operationalized into the two design goals presented in Table 2 to address the requirements "tailorable design" and "clear and uniform target groups" presented by Rostami *et al.* (2020a). These were treated as the primary requirements that we addressed. Having said that, eight additional requirements presented by Rostami *et al.* (2020a) were used as secondary requirements that are important when designing ISP content regardless of working with tailorable or monolith ISP design.

Requirement	Design goal	Design principle
Primary: Tailorable design Secondary: Actionable advice, adapted to the work practice, clarifying responsibilities, clear communicative objectives, clearly defined concepts, informed by laws, regulations and standards, goal alignment	1. To modularize ISP content	1. Use internally consistent and coherent ISP modules, because they enable a systematic decomposition of the ISP content 2. Use self-contained ISP modules because they are free-standing and reusable across multiple ISPs
Primary: Tailorable design, clear and uniform target groups Secondary: Clear structure	2. To create tailored ISP by reusing modules	3. Select ISP modules based on work tasks and assemble them to a tailored ISP because work tasks differ between roles and are means for tailoring

Table 2.
Requirements, design goals and design principles

The design and development phase focused on developing the conceptual model of policy components. As an empirical starting point for our conceptual modeling, we had access to a database of 159 ISPs from public agencies in Sweden. Still, modeling text documents is resource intensive. Consequently, we had to balance the resources available for modeling and arrive at a stable conceptual model. We, therefore, divided our modeling work into two steps:

(1) developing an initial conceptual model; and

(2) validating the model.

During the first step we selected the three most extensive ISPs that we had access to and used them as input to develop an initial conceptual model. Consequently, these ISPs were chosen because of their richness of data. The conceptual modeling of the ISPs took place during three workshops where all three authors participated. Duffy (1987) indicated that using more than one researcher with different and complementary skills can decrease potential bias and prevent the holistic fallacy in a study. The involvement of three researchers in these workshops can be seen to increase confidence in the modeling results. We focused on the structure among identified concepts that appeared in the ISPs. Thus, a natural means to structure this work was class modeling in terms of a unified modeling language (UML) class diagram. In addition, we used existing research on ISP design for the theoretical grounding of our conceptual model. As a result, an initial conceptual model was developed. Finally, to address the modularization and tailoring aspect of ISPs, we implemented the identified characteristics of SME presented in Table 1 in the design of the conceptual model. This implementation was not instrumental, and the design was adapted to the area of ISPs. We have summarized the essence of these implementations in the design principles presented in the rightmost column in Table 2.

During the second step, we validated the initial conceptual model using the ISPs from the database until we reached saturation (Glaser and Strauss, 1967). This meant, we stopped validating when modeling one more ISP would not add anything new to the conceptual model. To reduce researcher bias when selecting ISPs, we developed an algorithm to select ten ISPs from the available ISPs randomly for each validation iteration. We reached saturation after two iterations, which meant that we validated the conceptual model using 20 ISPs in total.

The first and third authors carried out a joint workshop to validate the conceptual model using the first of the randomly selected ISPs. The purpose of this workshop was to harmonize the way the validation was carried out. During this workshop, we used the constructs and associations in the conceptual model to sort the content of the ISP. In addition, things that could not be sorted using the conceptual model were noted and later considered as input for revising the model. The further validation work on the remaining ISPs from the first batch was divided between the two researchers. This work resulted in modifications of the conceptual model, where one new construct and some additional associations were identified. As a result, the first author carried out a second validation iteration with another ten randomly selected ISPs. No new classes or associations were elicited during this second iteration, although we decided to combine overlapping classes. Altogether this shows a stable conceptual model, where we have reached saturation. The refined model, with 13 classes, is presented in the Result section, where we also provide references to existing ISP design research, pinpointing the theoretical grounding of the model in addition to our empirical work and show how the model addresses the requirements in (Rostami *et al.*, 2020a).

The demonstration phase consists of two parts. First, the first and second authors used the conceptual model to elicit policy components from one of the ISPs from public agencies in Sweden that we had access to. Consequently, it is an empirical demonstration showing how policy components are self-contained and free-standing parts (i.e. meeting our first design goal). Second, the first and second authors used the elicited policy components to create two tailored ISPs targeting different target groups. This part of the demonstration shows how policy components can be reused across two tailored ISPs (i.e. meeting our second design goal). Goldkuhl and Karlsson (2020) argued that it is important to consider the maturity of the artifact when choosing the way of demonstration. We need to consider that this is the first version of the conceptual model, which means that we can expect design flaws to occur. Thus, executing this demonstration as a proof of concept is important before investing in software implementation and demonstrating tailoring as a proof of value and proof of use (Nunamaker and Briggs, 2011) in actual organizational cases.

The evaluation phase used the proof of concept demonstration as input. The evaluation targeted the two design goals and how the conceptual model helps address the primary requirements of our design work (see Table 1). Thus, it provides grounding of our design principles. During the evaluation, we explicitly focused on lessons learned from applying the conceptual model when modularizing and tailoring the selected monolith ISP.

Finally, the communication phase includes communicating the current version of the conceptual model and the results from the demonstration and evaluation in this paper. A shorter version of this work has previously been present at IFIP International Symposium on Human Aspects of Information Security and Assurance – HAISA 2022 (Rostami *et al.*, 2022).

5. Policy component – the conceptual model

5.1 Conceptual model

The conceptual model of policy components is shown in Figure 2 as a UML class diagram. The policy component consists of nine classes:

(1) Policy component;
(2) Policy statement;
(3) Actionable advice;
(4) Educational content;
(5) General content;
(6) Consequence;
(7) Concept;
(8) Goal; and
(9) Supplementary sources.

Between these classes, we find several labeled associations. In addition, the conceptual model includes four additional classes and several associations to enable tailoring. These classes are actor, role, information security policy and structure. In particular, the consist-of-association between policy component and information security policy is important because it shows how policy components are modeled as reusable modules across multiple ISPs.

In organizations, many different work tasks are carried out in relation to business processes. Thus, not all parts of an ISP are equally relevant for all roles and existing research recommends that ISPs are divided into several parts that target specific audiences (Wood, 1995; Simms, 2009; Cosic and Boban, 2010). Organizations define roles in order for

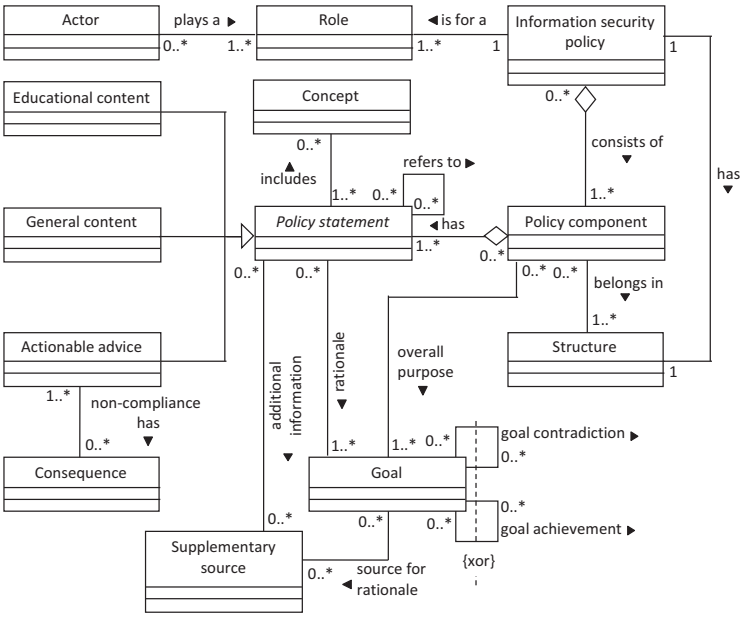

Figure 2.
Conceptual model for developing a computerized tool to design tailored ISPs

employees and other associated actors to know what is expected of them. Starting in the upper-left corner of Figure 2, an *Actor* is an individual associated with the organization, while a *Role* is a function played by an actor in the organization. Thus, actors playing the same role is a common ground for addressing the "clear and uniform target groups" requirement (Rostami *et al.*, 2020a). For example, at a hospital, an employee can play the role of a nurse in a ward. The model defines that actors included must have at least one role in an organization, but some roles may have no dedicated actors at a specific point in time.

A policy component can both guide and restrict work tasks associated with a specific role. Addressing the "tailorable design" requirement in (Rostami *et al.*, 2020a), i.e. making the ISP capable of being adapted to different target groups, we draw on SME research and structure guiding/restricting instructions into a set of modules, that can be reused to design ISPs that targets different roles. Thus, a policy component is a self-contained part of an ISP expressing rules that guide the protection of the organization's assets while executing a defined work task. The nurse exemplified above could have several defined work tasks and one of them could be to access a patient's medical record to provide care. The actionable advice (see below) in a policy component is prescribed to achieve one or more goals. A goal is a verifiable state of the world toward, which the policy component is directed. Goals can be derived from internal standards and/or supplementary sources, such as work instructions, laws and regulations. For example, one goal related to the exemplified work task above is to keep patient information confidential. By explicitly stating the goals of the policy components, it is possible to identify any goal conflicts that may create future noncompliance situations in cases where an employee does not prioritize these goals (Hedström *et al.*, 2011).

The policy components provide a set of policy statements to support an actor playing a role. Drawing on Höne and Eloff (2002b), a policy statement is direction-giving and guides toward the goal of the policy component. As shown in Figure 2, a policy statement is an

abstract class, which is specialized in three different types of policy statements (actionable, educational and general). These policy statements serve different purposes because existing research has shown that ISP parts have different communication objectives (Lindup, 1995; Karlsson *et al.*, 2017; Palmer *et al.*, 2001; Al-Mukahal and Alshare, 2015; Whitman *et al.*, 1999). Thus, this conceptual design addresses the "clear communicative objectives" requirement in Rostami *et al.* (2020a).

Actionable advice provides instructions and rules on how to execute a work task (Karlsson *et al.*, 2017). Consequently, an actionable advice defines what is allowed and what is not allowed regarding the specified work task (Davis and Olson, 1985). For example, when using medical records to provide care, one part of the actionable advice is to access a patient's medical records that the nurse provides care for only. It means that as a nurse you are not allowed to access all medical records. One main purpose of an ISP is to limit noncompliant behavior and actionable advice can be associated with one or more consequences. Drawing on deterrence theory (Herath and Rao, 2009; D'Arcy and Devaraj, 2012), a consequence is a specific sanction for not complying with the instructions and rules found in the actionable advice. In our running example, the policy component about using medical records to provide care should include consequences of accessing a patient record without having work-related reasons. Thus, the policy component could clearly state that the care provider always reports to the police when they suspect unauthorized access to patient records.

Educational content and general content serve a different purpose than actionable advice; these types of advice have no regulating purpose. Educational content provides information about information security where the purpose is to educate the actor. For example, the care provider can explain that activities in the electronic patient record system are logged and that these logs are audited regularly. By providing this information, the care provider can raise awareness of how the system works. Differentiating this type of content from actionable advice is in line with previous research, where Karlsson *et al.* (2017) have found that ISPs include both regulative and educational parts. Finally, general content provides information about the work task or the policy component itself. Thus, it serves the general purpose of informing the actor about different aspects of the organization, that does necessarily have to be related to information security. For example, the policy component about accessing a patient's medical record could include contact details of the system operator.

It is important that all actors using the ISP have a shared understanding of the terms used and what concepts they refer to Buthelezi *et al.* (2016), Koziel (2011), Höne and Eloff (2002a), Palmer *et al.* (2001). Information security and business terminology and concepts often come with certain complexity. Sometimes different terms refer to the same concept and what a concept may represent can differ between contexts. The policy component, therefore, includes the possibility to define concepts. A concept is a generic description of how something is conceived in the organization. In the example discussed above, confidentiality is a central concept to understand. Thus, a definition, such as "information is not made available or disclosed to unauthorized individuals, entities or processes" (ISO, 2017) could be included in a policy component about patient's medical records. The same concept can be associated with more than one piece of advice, such as actionable advice and educational content. This part of the conceptual model addresses the "clearly defined concepts" requirement in Rostami *et al.* (2020a).

Sometimes defining concepts is not enough. During our modeling work we came across that ISPs provided references to different sources where more information could be found about a topic. These sources served as background, for example showing why rules were

designed in a certain way. It means that in policy statements (i.e. actionable advice, educational content, general content) there is sometimes necessary to refer to other documents as a complement to the ISP. Thus, the different types of advice can include references to supplementary sources. A supplementary source is an artifact that contains additional information to specific advice. In our running example about accessing patients' medical records, a supplementary source could be the Patient Data Act (SFS 2008:355, 2008). Thus, supplementary sources acknowledge that ISPs need to be informed by, for example, laws, regulations and information security standards (Tuyikeze and Flowerday, 2014; Palmer *et al.*, 2001; Lopes and Oliveira, 2015; Rostami *et al.*, 2020a). These sources provide background information for the actionable advice that is provided in the policy component.

As shown in Figure 2, a tailored ISP made for a specific role consists of a selection of policy components. Being a self-contained module, a policy component includes all necessary information to guide an actor when executing a specified work task. The selection mechanism used to create a tailored ISP is the work task that a role executes, i.e. matching the work tasks that are performed by a role with the work task that policy components provide guidance on. Since a tailored ISP includes a set of policy components, the content of an ISP needs to be presented in a structured way (Palmer *et al.*, 2001; Koziel, 2011; Karlsson *et al.*, 2017; Höne and Eloff, 2002a, Corpuz and Barnes, 2010). Thus, to address the "clear structure" requirement in Rostami *et al.* (2020a), each ISP has a structure that organizes related policy components together.

6. Demonstration and evaluation of proof of concept

In this section, we demonstrate the policy component concept as a proof of concept. The demonstration is in two parts. The first part provides an internal view of one policy component, showing its content. We use the policy component class diagram in Figure 2 together with the ISP from a public agency in Sweden to elicit a reusable asset. We have focused on the work task of managing e-mails in the organization and how it is described in the ISP. Of course, one can argue that the choice is arbitrary. However, the importance lies in demonstrating where intertwined parts of an ISP have been separated and turned into a self-contained unit of instructions associated with a work task, i.e. making the existing ISP tailorable.

The second part of the demonstration shows the reuse of policy components in two tailored ISPs. Thus, this shows an external view of policy components, hiding their content. The purpose is to demonstrate how policy components can be selected and combined to create tailored ISPs targeting different roles based on the work tasks they execute. Here, we reuse the elicited policy component on managing e-mails to show how a policy component can be reused across ISPs.

6.1 Demonstration of proof of concept: a policy component

Since the existing (monolith) ISP which is used as a starting point for our demonstration was not designed with the policy component structure in mind, we had to move text around and rephrase some parts to create better flow in the text. Having said that, we strived not to change the meaning of the ISP content; still, the text below should not be interpreted as exact quotes from the original ISP.

Policy component: Managing e-mails

Goal: To govern the use of the agency's e-mail accounts.

Actionable advice: The e-mail account is for work purposes only. Received e-mails must be opened and read within one business day. For example, during an absence because of illness, vacation or other leave, you should grant a colleague the right to read incoming e-

mails. Note that an automatic reply is not considered sufficient. You may forward received e-mails to another e-mail address; however, replies to incoming e-mails shall be sent via the agency's e-mail address. You are not allowed to delete an incoming e-mail without first making sure what the content is. E-mails marked as spam must be inspected before deleting. Confidential information should not be sent via e-mail.

Consequence: In case of violation of these rules, the e-mail account will be terminated.

Educational content: Spam, also referred to as junk e-mail, is the practice of sending unsolicited messages in bulk by e-mail. There is a central e-mail filter that checks whether incoming e-mails might be spam or not to ease the burden of users. This task is carried out using a predefined set of rules. Spam messages are sent to a specific folder called "Spam." However, there is no definite way to define spam. Therefore, e-mails in this folder must be looked through before deleting. The use of e-mailing lists can be perceived as spam, and it is important to think about the relevance of the e-mail before sending it. The e-mail address represents the agency and thus affects the agency's reputation.

General content: Every staff receives an e-mail account according to the standard first-name.lastname@[agency].se. If there is more than one employee with the same first and last name, the first letter of the middle name will be used by the first-name.a.lastname@[agency].se

Concept: Confidential information is information that is made available to authorized individuals only.

Supplementary source: -

6.2 Demonstration of proof of concept: two tailored information security policies

In this part of the demonstration, we have created two tailored ISPs based on elicited policy components. Since the organization does not have tailored ISPs today, this demonstration shows what such a design would potentially look like. In Figure 3, we use an UML object diagram to illustrate the two tailored ISPs and parts of their content. Because of space limitations, we only show three policy components of each ISP. Still, it is enough to

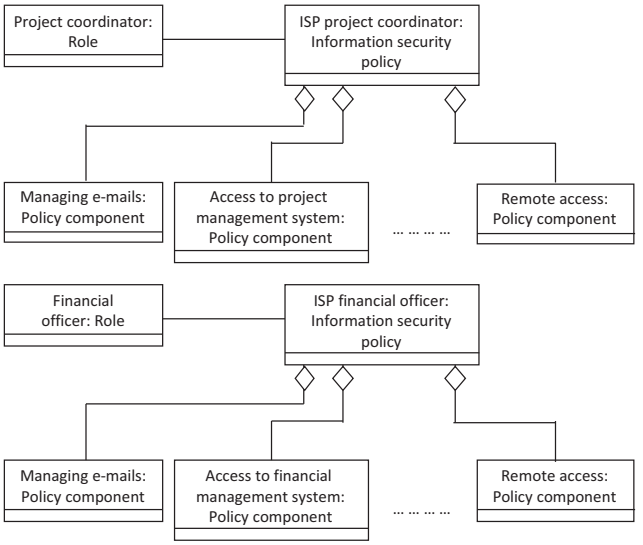

Figure 3.
Object diagram of two tailored information security policies

demonstrate the proof of concept, illustrating the basic principle of how the selection of policy components enables tailoring of ISPs and how the same policy component can be re-used across multiple ISPs. As it is shown in Figure 3, these two tailored ISPs target different roles. The uppermost ISP targets the project coordinator role, and the lowermost ISP targets the finance officer role. We have intentionally chosen two roles where it is reasonable to assume that they do not share many work tasks in their day-to-day work, which provides us with a possibility to show how the selection mechanism work when tailoring ISPs.

Starting to the left in both object diagrams, we find the policy component we elicited and presented in detail above, the Managing e-mails-component. When accessing the work task (i.e. our selection mechanism) this policy component addresses, it is a work task that all employees in the organization will execute. Therefore, this policy component is included in both tailored ISPs and shared across both roles. Next, we find policy components that are unique for each role, targeting the task of working with specific information systems. To do that, access is needed to each of these systems.

In the uppermost ISP, the second policy component from the left addresses access to the organization's project management system. We found that project coordinators use this information system to carry out day-to-day work tasks. However, finance officers do not use this system in any of their work tasks. Therefore, these regulations are not relevant to include in the ISP targeting financial officers. Instead, we find a policy component about accessing the financial management system, which manages the finances of the organization. It is an information system that the financial officers work with daily. This example shows how the difference in work tasks is used for the selection of policy components included in the ISPs.

Finally, rightmost in both object diagrams in Figure 3, we find a policy component shared across both ISPs. It targets how to work with the organization's information assets remotely. The policy component includes instructions on how to use the virtual private network software. This policy component is relevant for both exemplified roles and is necessary when accessing both the project management system and the financial system from a remote location. Thus, this shows that policy components can be included in the ISP to support other policy components.

6.3 Evaluation of proof of concept

In this subsection, we present lessons learned from our proof-of-concept demonstration. We do that by revisiting our design goals in Table 2. Our first design goal was to develop a conceptual model that supports modularized ISP content into self-contained and free-standing parts. The demonstration shows that we successfully were able to modularize an existing monolith ISP into several free-standing policy components. The detailed demonstration of the policy component in Section 6.1 shows that it is possible to develop free-standing and self-contained modules that provide meaningful guidance to the employee on how to deal with information security as an integrated part of the work task. Thus, this shows support for the first part of the second design principle (i.e. the policy components are free-standing).

As presented above, developing these policy components was not a simple copy-and-paste operation, since the content in monolith ISPs is intertwined. Thus, there was a need to move content around and rephrase text, to make the content fit the different classes in the policy component concept. Also, we should acknowledge that when assessing the policy components, sometimes we lacked content in the monolith ISP to fill all classes. Of course, one should not expect that all classes are used for all policy components, because sometimes a class might not be relevant. For example, in the detailed demonstration in Section 6.1, we

had no relevant information for supplementary source. Still, this demonstration provides support for the usefulness of the first design principle and that our conceptual model enables a systematic decomposition of the ISP content.

The second part of our demonstration targeted the second design goal, i.e. to develop a conceptual model that supports creating tailored ISPs by reusing modules. Our proof of concept shows that it is possible to select different policy components using work task as the selection mechanism. By assessing the work tasks that the two roles execute, we were able to select different policy components and assemble them into two tailored ISP. One challenge that we had was identifying the work tasks of each role, because the existing ISP did not include any thorough role descriptions; a few roles were covered in conjunction with pinpointing specific instructions. To some extent, this was expected because of the relevance-issue of monolith ISPs, i.e. that the same ISP is used for all employees. Of course, this made it challenging when selecting policy components for the different roles. Thus, we had to access other documents about role descriptions to identify a list of work tasks. In our demonstration, we relied on publicly available documents that described the roles we were interested in. It only allowed us to create simple lists of work tasks that each role execute. However, this type of information should be more easily available when tailoring is carried out in an organizational setting. Nevertheless, the demonstration shows support for the third design principle in Figure 3, i.e. that work task can be used as a selection mechanism. It also shows support for the latter part of the second design principle, i.e. that policy components are reusable across multiple ISPs. Furthermore, we expect this challenge to be less prominent when ISP content is being designed using policy components from the start and not being based on an existing monolith ISP.

7. Discussion and conclusion

This work makes a theoretical contribution with implications both for research and practice, which are discussed in the following. We end this section by pointing out the limitations and future work.

7.1 Implications for research

The proposed conceptual model is a theoretical contribution because the model together with the design principles can be considered as a new design theory (Gregor and Jones, 2007) for designing ISPs. This design theory represents a different way of thinking about ISP design where we, instead of designing a monolith ISP document, design and reuse demarcated policy components. As we showed in the previous section, policy components are provided in correspondence with work tasks that employees execute and a combination of one or more components forms distinctive ISPs for different roles. This new way of designing ISPs allows us to meet ISP design requirements previously mentioned in the literature without providing effective design solutions. For example, considering different target groups through a tailorable ISP or using a separate set of employee-oriented guidelines that more effectively communicate with employees are the ISP requirements that have been discussed in the literature (Cosic and Boban, 2010; Stahl *et al.*, 2012; Simms, 2009). Unlike other ISP requirements that have clear instructions about how to be attained, such as the breath, clarity and brevity (Goel and Chengalur-Smith, 2010), simple and understandable language (Ismail and Widyarto, 2016) and correct size (Höne and Eloff, 2002b), there has been no conceptual model that shows how tailorable ISPs could be designed. Thus, this study contributes to the extant ISP literature by presenting a conceptual model that makes designing tailored ISPs that target different employees possible.

The proposed conceptual model bears several short- and long-term implications for research. In the short term, the conceptual model can act as a foundation for developing software to design tailored ISPs. As it was said in the related research section, having software for designing ISPs has received limited attention from researchers (Rostami *et al.*, 2020b). Thus, the model can be considered as one step toward addressing this gap. In other words, the model can be applied to develop software that aids information security managers in modularizing and tailoring of ISPs.

Another short-term implication is that the conceptual model can be used as an analytical tool to understand the current status of ISPs in organizations. Researchers can analyze available ISPs to see which parts are missing and how they could be improved. For example, researchers can investigate to what extent existing ISPs pay attention to specific target groups and if the ISPs have been designed for different work tasks or not. Alternatively, researchers can investigate to what extent the consequences of noncompliance are made explicit. Based on their investigation results, researchers can decide whether there is a need to suggest changes to the ISPs and make related advice for organizations.

In the long term, having software that enables tailored ISPs and automates activities associated with such design activities will allow researchers to do new types of studies. For example, studies can assess the effect of such tools on the process of ISP development, i.e. construction, compliance and updating/monitoring. In the construction phase, researchers can investigate to what extent this type of software can ease the burden of information security managers when designing ISPs, something that today is considered a complicated and cumbersome task (Kinnunen and Siponen, 2018). Employees' reactions toward tailored ISPs and how these policies impact their understanding of ISPs and compliance with them can be explored in the compliance phase. Updating a tailorable ISP designed by this type of software might be different from the steps to update a monolithic ISP, considering that the latter type of update is often done manually. Updating a tailorable ISP might be simpler and faster since the indented parts that need to be changed are easily accessible through policy components. By using such software, it is not essential to go through the entire ISP to find the part that needs to be changed. Studies about the effects of this type of software on updating tailorable ISPs can be conducted in relation to the updating/monitoring phase.

Meanwhile, studies can be carried out by considering the whole ISP development process to understand how this type of software can change this process. Besides, Niemimaa (2016) showed in her ethnographic study that designing ISPs takes time, when considering the time from that managers decide to develop/update their ISP till it gets approved. In her study, it took about 15 months. Software that brings a new way of working might have the potential to shorten this time. Thus, there is an opportunity for researchers to examine the amount of time needed to design tailorable ISPs compared to the time needed to design monolithic ISPs manually.

The idea of the policy component embodied in the conceptual model came from the SME field (Henderson-Sellers *et al.*, 2014). Our study showed that it is possible to draw on the modularization concepts and design tailored ISPs for different roles in organizations. These modularization concepts have been used in the information security management field before, although not for this purpose. The method component format has been used when developing a method for information classification (Bergström *et al.*, 2020); our study can be considered another example of how SME concepts can inform information security management research.

Finally, this study also contributes to the body of literature on DSR by showing that design science is an appropriate approach to information security management. In our case, it has been used to develop the conceptual model. This study demonstrates how DSR can be

performed by following a DSR process model to develop an artifact in the information security management field. This effort is in line with Hevner *et al.* (2004) arguments that DSR should produce an artifact in the form of a construct, a model, a method or an instantiation.

7.2 Implications for practice

This study also has implications for practice. First, developing software based on the conceptual model is not only a research implication. Practitioners can use the model to develop software that can assist information security managers in designing tailorable ISPs. In contrast to existing, more process-oriented models and instructions on how to construct monolith ISP documents (e.g. ISO 27000 series), having such software enables the design of tailored ISPs based on the existing work tasks and roles at workplaces. Since the policy components are developed targeting employees' work tasks, such a tool could have the potential to simplify ISP design activities for information security managers. It is because information security managers' ISP development is divided into smaller parts (developing policy component) and thus provides a clear focus.

Second, considering that existing ISPs (that are developed manually without being tailorable) could be contradictory and cumbersome to follow for employees, using software for designing tailored ISPs offers the opportunity for information security managers to design more purposeful ISPs that might be less difficult to follow. Employees do not need to read the organization's monolith ISP document to understand which parts are relevant to their work tasks; instead, they read a more focused ISP that consists of policy components related to the tasks at hand. Using software as an assistant does not mean that information security managers have to start everything from scratch to design tailormade ISPs. As our demonstration shows, organizations could reshape their available ISPs and tailor them for different groups of employees. It might allow the information security managers to make their ISPs easier to follow among employees.

Third, it should be acknowledged that we intended to develop a conceptual model that can be applied across different types of organizations, i.e. being a generic model. It means that we searched for what ISPs in different organizations have in common. Of course, practitioners can take the model as it is to develop a supporting software. However, we encourage them to use their local knowledge when using the model as a starting point for developing such tools. It means that they should use those parts of the model that are in line with their local knowledge about their organizations and modify other pieces so that the developed tools suit their organizations.

7.3 Limitations and future research

The conceptual policy component model presented in this paper can be seen as a foundation for developing software that supports designing modularized and tailored ISPs. As with all studies, our study design has limitations. First, when developing the conceptual model, we analyzed three extensive ISPs from public agencies and used an additional 20 ISPs from public agencies for validation. Thus, during our design work, we focused on public agencies and did not use any ISPs from private companies and all the ISPs were from Swedish organizations. Consequently, we have not addressed any differences in ISP design across industry sectors and countries. It means that the design could be context bound, making it interesting to further demonstrate and evaluate the model using ISPs from other industry sectors and countries.

Second, we have demonstrated and evaluated the conceptual model as a proof of concept. It means that so far, the model has not been evaluated by practitioners in the information

security management domain, i.e. as proof of value or proof of use in actual organizational cases. The evaluation nevertheless contributes to knowledge by showing how the conceptual model can be used on an existing ISP to pursue the two design goals, i.e. the model can direct attention to certain aspects of ISPs that are important to reach these goals. However, more research is needed to demonstrate and evaluate the conceptual model to determine the proof of value and proof of use. To carry out such a demonstration, a software or at least a software prototype is needed to implement the proposed conceptual model. Otherwise, the ISP design work will still remain time-consuming and complex. As discussed under implications for research, future studies could evaluate proof of value and proof of use by assessing the applicability of such software (and indirectly the proposed model) when tailoring ISPs and the consequence on employees' awareness and understanding of ISPs and employees' compliance with ISPs.

References

Abraham, S. and Chengalur-Smith, I. (2019), "Evaluating the effectiveness of learner controlled information security training", *Computers and Security*, Vol. 87, p. 101586.

Adams, A. and Sasse, M.A. (1999), "Users are not the enemy", *Communication of the ACM*, Vol. 42 No. 12, pp. 41-45.

Albrechtsen, E. and Hovden, J. (2010), "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study", *Computers and Security*, Vol. 29 No. 4, pp. 432-445.

Al-Mukahal, H.M. and Alshare, K. (2015), "An examination of factors that influence the number of information security policy violations in qatari organizations", *Information and Computer Security*, Vol. 23 No. 1, pp. 102-118.

Bajec, M., Vavpotič, D. and Krisper, M. (2007), "Practice-driven approach for creating project-specific software development methods", *Information and Software Technology*, Vol. 49 No. 4, pp. 345-365.

Baskerville, R. and Siponen, M. (2002), "An information security meta-policy for emergent organizations", *Logistics Information Management*, Vol. 15 Nos 5/6, pp. 337-346.

Bergström, E., Karlsson, F. and Åhlfeldt, R.-M. (2020), "Developing an information classification method", *Information and Computer Security*, Vol. 29 No. 2, pp. 209-239.

Buthelezi, M.P., Van Der Poll, J.A. and Ochola, E.O. (2016), "Ambiguity as a barrier to information security policy compliance: a content analysis", *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, IEEE, pp. 1360-1367.

Cervera, M. (2015), "A Model-Driven approach for the design, implementation, and execution of software development methods", PhD, Universitat Politecnica de Vallencia.

Coertze, J. and Von Solms, R. (2012), "A model for information security governance in developing countries", *International Conference on e-Infrastructure and e-Services for Developing Countries*, Springer, Berlin, Heidelberg, pp. 279-288.

Coertze, J. and Von Solms, R. (2013), "A software gateway to affordable and effective information security governance in SMMEs", in Venter, H.S., Loock, M. and Coetzee, M., (Eds), *2013 Information Security for South Africa, 14-16 August*, IEEE, Johannesburg, pp. 1-8.

Coertze, J., Van Niekerk, J. and Von Solms, R. (2011), "A web-based information security management toolbox for small-to-medium enterprises in Southern africa", in Venter, H.S., Coetzee, M. and Loock, M. (Eds), *2011 Nformation Security for South Africa (ISSA 2011)*, IEEE, Johannesburg.

Corpuz, M. and Barnes, P.H. (2010), "Integrating information security policy management with corporate risk management for strategic alignment", *Proceedings of the 14th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2010)*.

Cosic, Z. and Boban, M. (2010), "Information security management—defining approaches to information security policies in ISMS", *IEEE 8th International Symposium on Intelligent Systems and Informatics*, IEEE, pp. 83-85.

D'arcy, J.D. and Devaraj, S. (2012), "Employee Misuse of information technology resources: testing a contemporary deterrence model", *Decision Sciences*, Vol. 43 No. 6, pp. 1091-1124.

Davis, G.B. and Olson, M.H. (1985), *Management information Systems: conceptual Foundations, Structure, and Development*, McGraw-Hill, New York, NY.

Dhillon, G. (2017), *Information Security - Text and Cases*, Prospect Press, Burlington.

Drechsler, A. and Hevner, A.R. (2018), "Utilizing, producing, and contributing design knowledge in DSR projects", in Chatterjee, S., Dutta, K. and Sundarraj, R.P. (Eds), *Designing for a Digital and Globalized World - 13th International Conference, DESRIST 2018*, Springer International Publishing, Cham, Schweiz, pp. 82-97.

Duffy, M.E. (1987), "Methodological triangulation: a vehicle for merging quantitative and qualitative research methods", *Image: The Journal of Nursing Scholarship*, Vol. 19 No. 3, pp. 130-133.

Enisa (2014), "ENISA Threat landscape 2014. Overview of current and emerging cyber-threats", European Union Agency for Network and Information Security.

Ernst and Young (2008), "Ernst and young 2008 global information security survey", Ernst and Young.

Ernst and Young (2010), "Borderless security - Ernst and young's 2010 global information security survey", Ernst and Young.

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.

Glaser, B.G. and Strauss, A.L. (1967), *The discovery of Grounded Theory: strategies for Qualitative Research*, Aldine, New York, NY.

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

Goldkuhl, G. and Karlsson, F. (2020), "Method Engineering as design science", *Journal of the Association for Information Systems (2020)*, Vol. 21 No. 5, p. 4.

Gregor, S. and Jones, D. (2007), "The Anatomy of a design theory", *Journal of the Association of Information Systems*, Vol. 8 No. 5, pp. 312-335.

Gritzalis, D. (1997), "A baseline security policy for distributed healthcare information systems", *Computers and Security*, Vol. 16 No. 8, pp. 709-719.

Harmsen, A.F. (1997), "Situational Method engineering", Doctorial Dissertation, University of Twente.

Harmsen, A.F., Brinkkemper, S. and Oei, H. (1994), "Situational method engineering for information system project approaches", in Verrijn Stuart, A.A. and Olle, T.W. (Eds), *IFIP WG8.1 Working Conference CRIS'94*, Maastricht, Elsevier, pp. 169-194.

Hedström, K., Kolkowska, E., Karlsson, F. and Allen, J.P. (2011), "Value conflicts for information security management", *The Journal of Strategic Information Systems*, Vol. 20 No. 4, pp. 373-384.

Henderson-Sellers, B., Ralyté, J., Ågerfalk, P.J. and Rossi, M. (2014), *Situational Method Engineering*, Springer-Verlag, Berlin Heidelberg.

Herath, T. and Rao, H.R. (2009), "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47 No. 2, pp. 154-165.

Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004), "Design science in information systems research", *MIS quarterly*, Vol. 28 No. 1, pp. 75-105.

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

Höne, K. and Eloff, J.H.P. (2002b), "What makes an effective information security policy?", *Network Security*, Vol. 2002 No. 6, pp. 14-16.

Hoppe, O.A., Van Niekerk, J. and Von Solms, R. (2002), "The effective implementation of information security in organizations", in Ghonaimy, M.A., El-Hadidi, M.T. and Aslan, H.K. (Eds), *Security in the Information Society - Visions and Perspective*, Springer, Boston, MA, pp. 1-18.

Ismail, W.B.W. and Widyarto, S.A. (2016), "Formulation and development process of information security policy in higher education", *1st International Conference on Engineering Technology and Applied Sciences*, Afyonkarahisar, Turkey.

ISO (2017), "ISO/IEC 27000:2017 information technology - Security techniques - Information security management systems – Overview and vocabulary", International Organization for Standardization (ISO).

Karlsson, F. (2013), "Longitudinal use of method rationale in method configuration: an exploratory study", *European Journal of Information Systems*, Vol. 22 No. 6, pp. 690-710.

Karlsson, F. and Ågerfalk, P.J. (2004), "Method configuration: adapting to situational characteristics while creating reusable assets", *Information and Software Technology*, Vol. 46 No. 9, pp. 619-633.

Karlsson, F. and Ågerfalk, P.J. (2009), "Towards structured flexibility in information systems development: devising a method for method configuration", *Journal of Database Management*, Vol. 20 No. 3, pp. 51-75.

Karlsson, F. and Wistrand, K. (2006), "Combining method engineering with activity theory: theoretical grounding of the method component concept", *European Journal of Information Systems*, Vol. 15 No. 1, pp. 82-90.

Karlsson, F., Hedström, K. and Goldkuhl, G. (2017), "Practice-based discourse analysis of information security policies", *Computers and Security*, Vol. 67, pp. 267-279.

Kinnunen, H. and Siponen, M.T. (2018), "Developing Organization-Specific information security policies", *Pacis 2018*, pp. 1-13.

Koziel, G. (2011), "Information security policy creating", *Actual Problems of Economics*, Vol. 12, pp. 126.

Kruger, H.A. and Kearney, W.D. (2006), "A prototype for assessing information security awareness", *Computers and Security*, Vol. 25 No. 4, pp. 289-296.

Lindup, K.R. (1995), "A new model for information security policies", *Computers and Security*, Vol. 14 No. 8, pp. 691-695.

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

Nash, K.S. and Greenwood, D. (2008), "The global state of information security", CIO Magazine (reprinted by PriceWaterhouseCoopers).

Niemimaa, E. (2016), "Crafting an information security policy: insights from an ethnographic study", *The 37th International Conference on Information Systems (ICIS 2016)*, AIS eLibrary, pp. Paper 6.

Nunamaker, J.F. and Briggs, R.O. (2011), "Toward a broader vision for information systems", *ACM Transactions on Management Information Systems*, Vol. 2 No. 4, p. 20.

Palmer, M., Robinson, C., Patilla, J. and Moser, E. (2001), "Information Security policy framework: best practices for security policy in the E-commerce age", *Information Systems Security*, Vol. 10 No. 2, pp. 1-15.

Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S. (2007), "A design science research methodology for information systems research", *Journal of Management Information Systems*, Vol. 24 No. 3, pp. 45-77.

Puhakainen, P. and Siponen, M. (2010), "Improving Employees' compliance Through information systems security training: an action research study", *MIS Quarterly*, Vol. 34 No. 4, pp. 757-778.

Pwc (2014), "The information security breaches survey - Technical report, Department for Business, Innovation and Skills (BIS), London, UK.

Pwc (2018), The Global State of Information Security Survey 2018, PriceWaterhouseCoopers.

Ralyté, J. and Franch, X. (2018), "Using Contextual goal models for constructing situational methods", in Trujillo, J.C., Davis, K.C., Du, X., Li, Z., Ling, T.W., Li, G. and Lee, M.L. (Eds), *Conceptual Modeling - 37th International Conference, ER 2018 Xi'an, China, October 22–25, 2018 Proceedings*, Springer, Cham, pp. 440-448.

Ralyté, J. and Rolland, C. (2001), "An Assembly process model for method engineering", *The 13th Conference on Advanced Information Systems Engineering (CAiSe '01)*.

Renaud, K. and Goucher, W. (2012), "Health service employees and information security policies: an uneasy partnership?", *Information Management and Computer Security*, Vol. 20 No. 4, pp. 296-311.

Rolland, C. and Prakash, N. (1996), "A Proposal For Context-Specific method engineering", in Brinkkemper, S., Lyytinen, K. and Welke, R. (Eds) *Proceedings of the IFIP TC8, WG8.1/8.2 Working Conference on Method Engineering on Method Engineering*, Chapman and Hall, Atlanta, pp. 191-208.

Rostami, E. (2019), "Tailoring policies and involving users in constructing security policies: a mapping study", in Furnell, S. and Clarke, N.L. (Eds) *Thirteenth International Symposium on Human Aspects of Information Security and Assurance, HAISA 2019, Nicosia, Cyprus, July 15-16, 2019, Proceedings*, University of Plymouth, Plymouth, pp. 1-11.

Rostami, E., Karlsson, F. and Gao, S. (2020a), "Requirements for computerized tools to design information security policies", *Computers and Security*, Vol. 99, p. 102063.

Rostami, E., Karlsson, F. and Gao, S. (2022), "Policy components - a conceptual model for tailoring information security policies", in Furnell, S. and Clarke, N. (Eds) *IFIP International Symposium on Human Aspects of Information Security and Assurance (HAISA 2022)*, Mytilenne, Greece.

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

Sandkuhl, K. and Seigerroth, U. (2019), "Method engineering in information systems analysis and design: a balanced scorecard approach for method improvement", *Software and Systems Modeling*, Vol. 18 No. 3, pp. 1833-1857.

Sfs 2008:355 (2008), "Patient Data act", in Affairs, M. O. H. a. S. (ed.).

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. and Downs, J. (2010), "Who Falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions", *The SIGCHI Conference on Human Factors in Computing Systems 2010*, Atlanta, USA, ACM, pp. 373-382.

Simms, D.J. (2009), "Information Security optimization: from theory to practice", *2009 International Conference on Availability, Reliability and Security*, Fukuoka, Japan, IEEE, pp. 675-680.

Siponen, M. and Iivari, J. (2006), "Six Design theories for IS security policies and guidelines", *Journal of Association of Information Systems*, Vol. 7 No. 7, pp. 445-472.

Siponen, M., Adam Mahmood, M. and Pahnila, S. (2014), "Employees' adherence to information security policies: an exploratory field study", *Information and Management*, Vol. 51 No. 2, pp. 217-224.

Stahl, B.C., Doherty, N.F. and Shaw, M. (2012), "Information security policies in the UK healthcare sector: a critical evaluation", *Information Systems Journal*, Vol. 22 No. 1, pp. 77-94.

Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005), "Analysis of end user security behaviors", *Computers and Security*, Vol. 24 No. 2, pp. 124-133.

Syamsuddin, I. and Hwang, J. (2010), "The use of AHP in security policy decision making: an open office calc application", *Journal of Software*, Vol. 5 No. 10, pp. 1162-1169.

Tuyikeze, T. and Flowerday, S. (2014), "Information Security policy development and implementation: a content analysis approach", *Haisa*, Plymouth University, UK, pp. 11-20.

Vermeulen, C. and Von Solms, R. (2002), "The information security management toolbox – taking the pain out of security management", *Information Management and Computer Security*, Vol. 10 No. 3, pp. 119-125.

Whitman, M.E. (2008), "Security Policy - From design to maintenance", in Straub, D.W., Goodman, S. and Baskerville, R. (Eds), *Information Security – Policy, Processes, and Practices*, M E Sharpe, New York, NY, pp. 123-151.

Whitman, M.E., Townsend, A.M. and Aalberts, R.J. (1999), "Considerations for an effective Telecommunications-Use policy", *Communications of the ACM*, Vol. 42 No. 6, pp. 101-108.

Wistrand, K. and Karlsson, F. (2004), "Method Components - Rationale revealed", in Persson, A. and Stirna, J. (Eds) *The 16th International Conference on Advanced Information Systems Engineering (CAiSE 2004)*, Springer, Berlin, pp. 189-201.

Wood, C.C. (1995), "Writing InfoSec policies", *Computers and Security*, Vol. 14 No. 8, pp. 667-674.

About the authors

Elham Rostami is doctoral student in Informatics at the Örebro University, Sweden. Her research interest focuses on information security management and in particular computerized tool-support for designing modular information security policies. Rostami has a master's degree in Informatics from the Örebro University. Elham Rostami is the corresponding author and can be contacted at: elham.rostami@oru.se

Fredrik Karlsson is Professor in Informatics at Örebro University, Sweden. His research interests focus on electronic government, information security, tailoring of systems development methods, and method rationale. His research has appeared in a variety of information systems journals such as *European Journal of Information Systems, Government Information Quarterly, Information Management and Computer Security, Strategic Journal of Information Systems* and *Scandinavian Journal of Information Systems*.

Shang Gao is Associate Professor in Information Systems at the School of Business, Örebro University, Sweden. He obtained his PhD (2011) in information systems from Norwegian University of Science and Technology (NTNU). His research interests include mobile information systems, technology diffusion, business process modeling and information systems modeling and requirement engineering. He has published more than 60 refereed papers in journals, books and archival proceedings since 2006.