DOCTORAL THESIS

Making the Dead Alive

Dynamic Routines in Risk Management

Martin Lundgren

Information Systems

LULEÅ UNIVERSITY OF TECHNOLOGY

LULEÅ
UNIVERSITY
OF TECHNOLOGY

Making the Dead Alive

Dynamic Routines in Risk Management

Martin Lundgren

Luleå University of Technology
Department of Computer Science, Electrical and Space Engineering
Division of Digital Services and Systems

Printed by Luleå University of Technology, Graphic Production 2020

ISSN 1402-1544
ISBN 978-91-7790-563-9 (print)
ISBN 978-91-7790-564-6 (pdf)

Luleå 2020

www.ltu.se

Acknowledgments

As I am sitting here, during a global pandemic, staring out over a rainy Gothenburg where I have been stranded for well over a month, what remains is the daunting task of formulating my acknowledgments. Daunting, mostly because it neatly boils down roughly a decade of work, colleagues, and friends to a few heartwarming, honest—albeit slightly cheesy—gratitudes.

Now, who to blame? First and foremost, I would like to express my warmest gratitude to my supervisors, colleagues, and friends Prof. Åsa Ericson and Dr. Johan Lugnet, whose guidance, insights, and feedback have been invaluable in stitching this dissertation together. Thanks for putting up with me, your energy and patience has been nothing short of impressive. I count myself lucky to have had you there by my side, engaging (with) me in my area of research, making this journey possible, and securing relevant projects, such as the Interreg Nord project CYNIC which has provided a good platform to interact with companies, and to disseminate the results to a wider audience. Somehow, along the way, I am pretty sure I have managed to peek your interests in information security… erm, sorry about that.

While on the topic on making things possible, I must thank all of my friends and colleagues—both old and new—for making this journey so much more enjoyable. I look forward to continue spending time—hopefully more so hereafter—and working with you all. But this journey also started long before I enrolled in the doctoral program at Luleå University of Technology, and before I took my Master's or even Bachelor's degree. Indeed, it has—especially at times—been quite a long adventure, complete with people seemingly set on making it clear that school perhaps is not something for me. Luckily, I have had family and loved ones in my life to support me all the way.

Therefore, finally, I would like to dedicate this work to those closest to me in life—and should you be reading this and wonder if you are one of them, you probably are. Thank you …….

(insert name here)

28 April 2020,
Martin Lundgren

Abstract

Risk management in information security is relevant to most, if not all, organizations. It is perhaps even more relevant considering the opportunities offered by the digitalization era, where reliably sharing, creating, and consuming information has become a competitive advantage, and information has become an asset of strategic concern. The adequate protection of information is therefore important to the whole organization. Determining what to protect, the required level of protection, and how to reach that level of protection is considered risk management, which can be described as the continuous process of identifying and countering information security risks that threaten information availability, confidentiality, and integrity.

The processes for performing risk management are typically outlined in a sequence of activities, which describe what organizations should do to systematically manage their information security risks. However, risk management has previously been concluded to be challenging and complex and as something that must be kept alive. That is, routines for performing risk management activities need to be continuously adapted to remain applicable to organizational challenges in specific contexts. However, it remains unclear how such adaptations happen and why they are considered useful by practitioners, as there is a conspicuous absence of empirical studies that examine actual security practices.

This issue is addressed in this thesis by conducting empirical studies of governmental agencies and organizations. This was done to contribute to an increased understanding of actual security practices. The analysis used for this study frames formal activities as 'dead routines,' since they are constructed as instructions that aid in controlling performance, such as risk management standards. Practitioners' performance, experience, and understanding are denoted as 'alive routines,' as they are flexible and shaped over time. An explanation model was used to elaborate on the contrast between dead—controlling—and alive—shaping—routines of risk management.

This thesis found that when dead and alive routines interact and influence each other, they give rise to flexible and emergent processes of adaptations, i.e., dynamic routines. Examples of dynamic routines occurred in response to activities that were originally perceived as too complex and were adapted to simplify or increase their efficiency, e.g., by having a direct relation between security controls and asset types. Dynamic routines also appeared as interactions between activities in response to conflicting expectations that were adjusted accordingly, e.g., the cost or level of complexity in security controls. In conclusion, dynamic routines occur to improve risk management activities to fit new circumstances.

Keywords

Risk management, information security, routine, practice, asset identification, risk analysis, risk treatment, organizational aspects.

Thesis

This thesis comprises an introductory part and the following appended papers:

Paper A
Lundgren, M. (2020) 'Rethinking capabilities in information security risk management: a systematic literature review,' *Int. J. Risk Assessment and Management,* Vol. 23, No. 2, pp.169–190.

Paper B
Lundgren, M. and Bergström, E. (2019) 'Dynamic interplay in the information security risk management process,' *Int. J. Risk Assessment and Management*, Vol. 22, No. 2, pp.212–230.

Paper C
Bergström, E., **Lundgren, M.**, and Ericson, Å. (2019) 'Revisiting information security risk management challenges: a practice perspective,' *Information & Computer Security*, Vol. 27, Issue: 3, pp.358–372.

Paper D
Bergström, E., **Lundgren, M.** (2019) 'Stress Amongst Novice Information Security Risk Management Practitioners,' *Int. Journal on Cyber Situational Awareness*, Vol. 4, No. 1, pp.128–154.

The following papers are related to this thesis, but not included:

Lundgren, M. (2016, August) 'What's in the box? – A Review on Risk Management Routines and Capabilities in Information Security,' In *39th Information Systems Research Conference in Scandinavia* (IRIS), Ljungskile, Sweden

Lundgren, M. (2018, April) 'Making Information Security Research Great Again: Assumptions and Practical Aspects of Case-Study Research in Information Security,' In *2nd International Symposium on Small-scale Intelligent Manufacturing Systems* (SIMS), IEEE, Cavan, Ireland.

Lundgren, M., and Bergström, E. (2019, June) 'Security-Related Stress: A Perspective on Information Security Risk Management,' In *2019 International Conference On Cyber Security and Protection of Digital Services* (Cyber Security), IEEE, pp.273-280, Oxford, UK.

Contents

1 Introduction

1.1 Importance and Problem

Information security risk management—hereafter risk management—has been a topic of ongoing research since the 1970s (Fenz and Ekelhart 2011) and has become increasingly relevant alongside the challenges and opportunities of the digitalization era (Schirrmacher et al. 2018). Risk management is theoretically described as a continuous process to identify and protect the confidentiality, integrity, and availability of information assets to reach an acceptable level of risk (Gerber et al. 2001; Spears and Barki 2010; Whitman and Mattord 2014). Securing information has undergone a transformation since the 1970s from mainly being understood as a precise, technical problem emphasizing computer properties to becoming a part of organizational governance. Thus, information is emphasized as an important competitive asset and is therefore of strategic concern (Gerber et al. 2001; Hedström et al. 2011; von Solms 2006; von Solms and von Solms 2004). Delayed, unavailable, inaccurately manipulated, or leaked confidential information, causes serious setbacks to organizations (Gerber and Von Solms 2001). Identifying valuable information and protecting it with safeguards—i.e., security controls—is therefore highly relevant to most, if not all, organizations and key to risk management. Acts and incidents that negatively impact information or its intended usage could therefore be considered a threat to the whole organization. However, threats can, to varying degrees, be managed and thereby controlled. By better understanding vulnerabilities—i.e., the circumstance that made the threat possible in the first place—the source, odds, and impact of the threat can be reduced or removed.

Over the years, developments in risk management made by researchers and practitioners alike have led to various standards, guidelines, and frameworks—hereafter simply referred to as formalized processes—that may guide organizational strategies in performing activities, i.e., helping them to focus on ways to systematically identify and protect their information assets (Al-Ahmad and Mohammad 2013; Siponen and Willison 2009; Whitman and Mattord 2014). Formalized processes are therefore vital since they describe generic templates for risk management work routines. However, little is known about how organizations actually protect themselves (Baskerville et al. 2018), as there is a conspicuous absence of empirical studies regarding security practices due to their sensitive nature (Cram et al. 2019; Hsu 2009; Kotulic and Clark 2004; Webb et al. 2014). This absence can be seen in the uncertainty surrounding how described patterns of activities in formalized processes are adapted to fit a particular organization and how they are practised in actual work routines (Siponen and Willison 2009). It has been concluded that such organizational fit is an ongoing effort of reflective and adaptive practitioners that can override formalized processes in practice (Njenga and Brown 2010, 2012). This indicates that risk management is a challenging process which work routines must be kept alive and shaped over time as practitioners adapt their strategy to organizational challenges and specific contexts (Coles-Kemp 2009; Niemimaa 2016).

While it is tempting to assume that formalized processes will control the performance of risk management activities, they simply provide a limited guidance of action and therefore can not determine performance since context varies (Pentland and Feldman 2005). Formalized processes can, in this sense, be described as controlling but dead (Cohen 2007). It might even be possible to argue that formalized processes can be viewed as ends, rather than means, in the sense that fulfilling a particular risk management standard is equivalent to having good information security (Webb et al. 2013). Risk management is thus in danger of being viewed as a final product rather than a learning process (Wangen and Snekkenes 2013). Such a limited perspective may be based on two organizational standpoints. The first standpoint holds that formalized processes can be readily understood and will be correctly adopted by all practitioners. However, research has discovered that there are many different perspectives on risk management and its process, which has led to some confusion about what activities should be included (Gerber and Solms 2005; Pan and Tomlinson 2016; Shedden et al. 2016). The second standpoint presumes that formalized processes operate well when implemented. However, research has concluded that social and organizational differences must be considered in this assumption, and there is no single approach that fits every situation (Al-Ahmad and Mohammad 2013; Choobineh et al. 2007; Williams 2007).

1.2 Purpose

Risk management can therefore be theoretically described through formalized processes as controlling, dead instructions dictating which activities to perform. However, it is also a process that is alive and shaped over time, as practitioners adapt their strategies for performing risk management activities to fit specific organizational challenges in specific contexts. Understanding the interplay between controlling—dead routines—and shaping—alive routines (Cohen 2007)—is central for adaptations of strategy and for the continuous improvement of risk management. While research has noted a contrast between dead and alive routines—i.e., that formal processes support control and that actual performance gives rise to new strategies—it is still unclear how these adaptations of strategy happen and why they are considered useful by practitioners. The purpose of this thesis is therefore to explore how and why these adaptations occur in risk management.

1.3 Delimitation

To study adaptations, the scope of risk management was narrowed down to three core activities, namely, asset identification, risk analysis, and risk treatment. This was done to unify different risk management processes to move focus away from the processes themselves and towards how the activities were carried out. With respect to adaptation, the study uses an explanation model adapted from the concept of dead and alive routines (Cohen 2007) and organizational routines (D'Adderio 2011; Pentland and Feldman 2008). The focus has thereby been placed on risk management activities performed within the context of organizations.

The study took place in close relation with government agencies and public sector organizations in Sweden. The organizations represent different functions within society and different relationships to risk management work, as well as different levels of maturity in risk management. Data were collected through interviews and observations.

2 Theoretical Domain

2.1 Information Security

Information security aims to protect information—e.g., facts, ideas, and knowledge—regardless of the medium or form it is in—be it physical or digital, in people's minds, or in verbal or visual forms of communication—from "*unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability.*" (ISO/IEC 27000 2018; Nieles et al. 2017, p. 2; von Solms and von Solms 2018) Confidentiality, integrity, and availability are commonly referred to as the CIA-triad, or CIA-triangle, and are agreed to be the principles for which aspects of information should be protected (von Solms and van Niekerk 2013). In this regard, *confidentiality* refers to information only being available to authorized people with sufficient privileges; *integrity* refers to information being whole, that is to say, complete and not corrupted by any unauthorized, unintentional, or wrongful manipulation or deletion; and *availability* refers to information being accessible and in a usable format, when needed (Whitman and Mattord 2014). Information security is the preservation of confidentiality, integrity, and availability (ISO/IEC 27000 2018).

2.2 Risk Management

Information security is not static but requires "*continuous monitoring and management to protect the confidentiality, integrity, and availability of information as well as to ensure that new vulnerabilities and evolving threats are quickly identified and responded to accordingly.*" (Nieles et al. 2017, p. 10) These requirements also align closely with definitions of risk management (Wangen et al. 2018; Wangen and Snekkenes 2013) and are therefore often seen as the core of the management of information security (Blakley et al. 2001; Spears 2005; Yang et al. 2016). That is, while information security represents the general domain of protecting information, and the carrier of theories for what it means to protect information—i.e., the CIA triad—, risk management drives those theories into practice by identifying and prioritizing what to protect and how it should be protected (ISO/IEC 27000 2018). As such, risk management is a process consisting of a set of organized activities within the domain of information security (ISO/IEC 27000 2018; Nieles et al. 2017).

2.2.1 Assets, threats, vulnerabilities, risks, and controls

Risks within information security consist of three components: assets, threats, and vulnerabilities (Gerber and Von Solms 2001; Ozkan and Karabacak 2010). Assets are information resources, e.g., intellectual property, employee details and financial details (ISO/IEC 27000 2018). As with any other organizational resource of value, assets must be adequately protected from threats. Threats can be defined as any potential cause of unwanted incidents that may cause harm (e.g., damage or otherwise compromise) an

organization's assets (ISO/IEC 27000 2018; Peltier 2010). The source of a threat can vary (Nieles et al. 2017; Whitman and Mattord 2014), including the following:

- natural, e.g., fire, flooding, lightning,
- human, e.g., accidents, unauthorized access, theft, or
- technical, e.g., malicious code, hardware failure, software bugs

For a threat to be effective, however, there must be a vulnerability that it can exploit. A vulnerability is what enables a threat to become an actual incident. It can be a weakness in a system, procedure, or environment that leaves that component of the organization susceptible to adversarial or non-adversarial threats, coming from within or outside of the organization (Nieles et al. 2017). To counter or treat a risk, security controls—also known as counter measures or safeguards—can be implemented. A security control can be defined as "*any process, policy, procedure, guideline, practice or organizational structure, which can be administrative, technical, management, or legal in nature which modify information security risk*." (ISO/IEC 27005 2013, p. 2)

There are a few common categories of security controls. These categories are often referred to as treatment or mitigation strategies. Although different strategies go by different names, depending on their particular risk management approach (e.g., ISO/IEC 27005 2018; NIST SP 800-30 2012; Whitman and Mattord 2014), they can be summarized as the following categories: defend, transfer, mitigate, accept, and avoid (ISO/IEC 27000 2018; Peltier 2010; Whitman and Mattord 2014), where:

- The *defence* strategy aims at removing or reducing the risk of a vulnerability and may include security controls such as security policies, training, access controls, and technical safeguards (Whitman and Mattord 2014).
- The *transfer* strategy aims at shifting the risk to other areas of the organization or outside of the organization, and may include security controls such as outsourcing, the purchase of insurance, and service level agreements with third parties (Peltier 2010; Whitman and Mattord 2014).
- The *mitigation* strategy aims to reduce the impact to the organization if a vulnerability is exploited and is thus a reactive strategy. This strategy includes security controls such as disaster recovery plans, incident response plans, and business continuity plans (Whitman and Mattord 2014).
- The *acceptance* strategy involves, as its name suggests, accepting the risk without further modification. It could be the most appropriate strategy if, for example, the cost of controlling the risk is deemed to be higher than its estimated benefit (Whitman and Mattord 2014).
- The *avoidance* strategy refers to moving or discontinuing the asset from the environment that it was in, and thereby removing the risk altogether (ISO/IEC 27005 2018; Peltier 2005).

The process of identifying and prioritizing information assets, probable threats and vulnerabilities and determining what treatment strategy to use to implement appropriate security controls to manage risks is risk management (ISO/IEC 27000 2018).

2.2.2 Formalized processes

In 2011, a study estimated that there are more than 200 different risk management processes (Saleh and Alfantookh 2011), each developed to meet its own particular needs and objectives (Shameli-Sendi et al. 2016). As such, they often differ in particular process

parts, and have subtly different definitions (Pan and Tomlinson 2016). Although the formalized processes differ, they also commonly share some goals, such as the identification of assets, the analysis of risks, and the treatment of risks to bring them to an acceptable level (Saleh and Alfantookh 2011). Three common industry risk management processes (Silva and Jacob 2018) are NIST SP 800-30 (2012), ISO/IEC 27005 (2018), and OCTAVE Allegro (Caralli et al. 2007).

NIST SP 800-30 (2012) is suited for large organizations and government agencies and offers a comprehensive guide to implementing risk management (Hashim et al. 2018). Its process relies heavily on the skills and experience of security analysts, technical experts, and system owners to evaluate and manage the risks in IT systems (Kunder and Clarke 2013; NIST SP 800-30 2012). Its process consists of the following four parts. First, framing risk aims to set the scope and boundaries for what is to be protected. Thus, framing risk begins by identifying critical assets, and then clarifies how threats, vulnerabilities, impacts, and the probability of incidents occurring should be defined and prioritised. Next is the risk assessment, as defined in NIST SP 800-39 (2011). Based on the definition formulated during the 'framing' part of the process, the risk assessment aims to identify the threats and vulnerabilities of assets, estimate how likely incidents are to occur, and what the impact could be. The output of this activity is a series of potential risks, which serves as input for the response part of the process, to determine the most appropriate treatment strategy. The last part of the process is risk monitoring, which aims to continuously analyse whether treated risks or new assets are within an accepted level (NIST SP 800-30 2012). The NIST SP 800-30 (2012) process parts are listed below:

- Framing risk
- Assessing risk
- Responding to risk
- Monitoring risk

Other risk management processes, such as the ISO/IEC 27005 (2018, p. 1), is similar in structure to NIST SP 800-30 (2012) but designed to fit "*all types of organizations.*" The ISO/IEC 27005 process consists of the following parts: context establishment, which aims to first define how to evaluate risk and potential impact, and then to set the scope and boundaries for what to protect. Next is the risk assessment, which consists of three sub-parts: risk identification, risk analysis, and risk evaluation that aims at identifying assets, their impact on the organization, possible threats to these assets, and their vulnerabilities. This information serves as the input for the risk treatment part of the process, which determines which treatment strategy should be applied based on the risk assessment. The last part in the process is risk monitoring and review, serving as a feedback operation, aiming to continuously analyse whether the treated risks, as well as new assets, are within an accepted level. In addition, communication and consultancy runs parallel to the other parts of the process (ISO/IEC 27005 2018). The ISO/IEC 27005 (2018) process parts are listed below:

- Context establishment
- Risk assessment
- Risk treatment
- Risk monitoring and review
- Communication and consultancy

The OCTAVE Allegro (Caralli et al. 2007) process is specifically developed to be a light version of risk management and offers a self-assessed approach intended to be applied by employees within an organization as a dedicated team. Its process consists of the following eight parts. First, a risk measurement criteria is established, which aims to define risk evaluation criteria and set the scope and boundaries for areas to protect in the organization. The next part focuses on developing information asset profiles, meaning that valuable assets are identified for further analysis and documented, along with important security requirements for that asset. OCTAVE Allegro uses and identifies information asset containers to group assets into. Containers can be technical, physical, or human and are defined as the locations where identified assets are stored, transported, and processed. The next part of the process aims to identify areas of concern. Here, the first real world scenarios that come to mind as being able to pose a threat to the identified information assets are noted. These scenarios are then further detailed and grouped together during the following step, the identification of threat scenarios. The impacts and consequences of the identified threats are then investigated during the next two steps, identification and analysis of risks, respectively. Finally, each resulting risk is prioritised, and an appropriate mitigation approach is selected and implemented (Caralli et al. 2007). The OCTAVE Allegro process parts are listed below:

- Establish risk measurement criteria
- Develop information asset profile
- Identify information asset containers
- Identify areas of concern
- Identify threat scenarios
- Identify risks
- Analyse risks
- Select mitigation approach

Research has led to the suggestion of additional risk management processes (Amraoui et al. 2019; Pan and Tomlinson 2016). The following five-part process is an example (Straub and Welke 1998), in which the first part aims at recognizing security problems and formulates potential security problems and issues with respect to an organization's information systems. These identified areas of concern are then incorporated into a risk analysis, in which potential threats exploiting these problems and issues are identified to establish and prioritise risks. The identified risks then serve as the input for the next part of the process, the generation of alternatives. This part aims to generate security solutions to meet the risks that were previously identified. Next is the decision part, in which the final security solutions are selected and prioritised. Finally, the selected security solutions are then implemented in the prioritised order. The risk management process parts are listed below:

- Recognition of security problems
- Risk analysis
- Generation of alternatives
- Decisions
- Implementation

It has been proposed that other processes benefit from following the six-sigma process (Saleh and Alfantookh 2011), consisting of the following five parts. First is the

definition part, which aims to establish the scope and context and to map the current situation with regards to existing organizational assets, threats, vulnerabilities, and controls, as well as to specify the assets' locations, owners, sources of threats, and security requirements. The output from this step represents the current state of the information security considerations in the organization and serves as the input into the measurement part of the process. During the measurement part, assessments of the current state of the assets and their threats, vulnerabilities, and controls are compiled for each asset. The output of the assessment step then serves as the input for the analysis part of the process. Here, potential gaps between current security controls (as assessed in the measurement part of the process) and the required state of security (as defined earlier in the process) are identified. Each gap is further considered in the improvement part, in which a plan of action for closing each gap is developed to achieve the required state of security. Finally, the control part of the process selects, implements, monitors, and documents each improvement plan. The six-sigma process parts are listed below:

- Define
- Measure
- Analyse
- Improve
- Control

CORAS is another example of risk management (Djordjevic et al. 2002; Fredriksen et al. 2002). Originating from a research and technology development project, CORAS outlines a five-part process. Context identification, which is the first part, aims to identify areas of concern and security requirements, as well as identify and evaluate assets (Djordjevic et al. 2002; Wangen et al. 2018). The next part is risk identification, which aims to recognize threats and vulnerabilities to the identified assets and areas of concern. Each of the threats identified are then assessed in a risk analysis and assigned a value to indicate their level of potential consequences and their likelihood of occurrence. The resulting level of threat and consequence are then considered in the risk evaluation part of the process to determine and prioritise the level of risk for each threat. The resulting series of prioritized risks then serves as the basis for the risk treatment, in which different treatment options are identified, assessed, and selected (Djordjevic et al. 2002; Fredriksen et al. 2002). The CORAS process parts are listed below:

- Identify context
- Identify risks
- Analyse risks
- Risk evaluation
- Risk treatment

2.2.3 Challenges

Formalized processes are valuable tools, as they organize risk management activities into sequences of distinct parts, thus providing instructions for a strategy to accomplish the work. However, they have also been criticized for concentrating mainly on generic guidance and output, while leaving the practitioner to determine the content of those parts (Shameli-Sendi et al. 2016; Siponen 2006). Research has identified a number of related challenges regarding the practice of risk management (Fenz et al. 2014; Wangen and Snekkenes 2013). Several of these relate to the required skills and knowledge

needed to perform risk management activities, as well as to interpret the results (Kunder and Clarke 2013). This has resulted in formalized processes often being perceived as too complex and as requiring help from outside consultants to implement and achieve (Peltier 2010). The complexity can, for example, be seen in the challenges associated with information valuation. To adequately protect information assets, an asset's value to the organization is commonly established first, so as not to over- or under-protect the asset (Wei et al. 2018). However, the evaluation of information has been shown to be difficult to agree upon between practitioners due to differences in perspectives (Kaarst-Brown and Thompson 2015). Therefore, there is the possibility of causing erroneous results further along in the process due to an inaccurate asset evaluation (Foroughi 2008), since asset evaluation is one of the cornerstones of risk management (Wangen et al. 2018). Even when given clear instructions for how to evaluate information, the subjectivity in valuations causes different practitioners to value assets differently (Mersinas et al. 2016).

Similarly, the identification and the evaluation of risks have also been shown to be difficult to carry out and can sometimes lead to worse results—e.g., more time consuming and costly than what is justifiable—for an organization than not having risk management in place at all (Douglas 2009). To overcome some of the challenges associated with risk identification, checklist-based methods have been proposed. However, because of their generic nature, checklists offer a limited view of threats facing the organization (Shedden et al. 2010) and therefore miss risks that arise only in specific contexts, e.g., as a result of poor work practices (McEvoy and Kowalski 2019). In addition, checklists can also result in practitioners choosing and addressing non-existing risks from the list, possibly due to a lack of information security experience or skills (Wei et al. 2018). Thus, practitioners end up spending time and resources on risks that may never occur. However, even among practitioners with considerable security experience, risk evaluations have been shown to differ. Security professionals have been found not only to evaluate risks differently from one another but also to manage and treat them differently due to preferences, different standpoints, and previous experiences (Mersinas et al. 2016).

Therefore, several formalized processes have been suggested using quantitative methods based on, for example, statistical data to better perform accurate risk evaluations. However, in practice, there is little information regarding how to obtain such quantitative data (Taylor 2015; Wangen et al. 2018). Furthermore, the use of quantitative methods requires organizations to have personnel with the necessary skills to apply these methods—often requiring extensive mathematical calculations—which organizations do not always have (Ozkan and Karabacak 2010). In addition, it also assumes practitioners are rational and are able to interpret and use the data correctly to identify adequate security controls. However, research has shown that risk management practitioners do not always act rationally but often base their decisions on heuristics and optimistic perceptions (Taylor 2015).

2.3 Dead and Alive Routines

There is a difference between the theoretical description of formalized processes and how they are performed in practice (Miner 1990; Pentland 2003). Because circumstances not covered by the formalized process sometimes arise, practitioners may

have to be creative and develop new ways of performing activities to overcome those challenges (Miner 1990). In this sense, practitioners are understood to act knowledgeably as they introduce adaptations to their work routines (Higgins 2009; Pentland 2003). Therefore, while formalized processes provide a sound strategy for what to do, risk management cannot solely be understood by their instructions. Rather, formalized processes should be viewed as a pattern of activities that are shaped over time as circumstances change and as new experiences are drawn from and applied anew in practice, i.e., what can be referred to as 'knowings.' (Orlikowski 2002) In other words, it is in practice "*that knowledge comes to life, stays alive, and fades away.*" (Nicolini et al. 2004, p. 26)

The term 'knowing,' is in this case used as a verb to indicate actions, or enactment, rather than factual 'knowledge.' This illustrates an important distinction between the former, as an activity that takes place in practices and unfolds over time; and the latter, which can be conceptualized as a specific concept, that can be easily shared and codified (Gherardi 2009; Nonaka et al. 2000). For example, formalized processes can be described as a set of explicit instructions manifested in and codified on, for example, paper, software, and tools (D'Adderio 2011). However, risk management has been reported as being difficult to implement and perform (Maneerattanasak and Wongpinunwatana 2017; Osborn and Simpson 2018). These difficulties appear even with additional supporting tools, such as software, to help guide the process (Gritzalis et al. 2018;Yang et al. 2016). Thus the implementation and performance of risk management has proven to be challenging, particularly for security novices who have little or no previous experience and know-how (Wangen 2017). On the other hand, practical training and experience have been found to be key in obtaining the necessary know-how (Haqaf and Koyuncu 2018). Knowing how to perform the instructions outlined in the formalized processes thus rises in the practice itself (Orlikowski 2002), which is learned and shaped through participation. As such, there is a relationship between knowing how things get done and knowing what to do (Cox 2012; D'Adderio 2011).

The word 'routine' can be defined as the framework used to explain the interrelations between the formulated strategy of activities and the actual, specific performance of activities, and their relation to formalized processes (Pentland and Feldman 2005). For some time, formalized processes have been presented as opaque, lifeless objects that lie outside of routines and gravitate them towards the automatic, mindless effort that for so long has been the idea of routine work (D'Adderio 2011). This instructional view of routines suggests that they are rigid, mindless, and can be explicitly stored, and that the creation of new work routines is a matter of introducing new instructions, rules, checklists, or software (Pentland and Feldman 2008). Similar approaches have commonly been proposed for the implementation of risk management activities in organizations (Dhillon and Backhouse 2001; Njenga and Brown 2012).

This instructional view of routines can be defined as a 'dead' routine (Cohen 2007), conducted as controlled activities. Dead means not so much inconsequential, but rather that it promotes a hardened, or solidified, approach (D'Adderio 2011). The importance of dead routines can be seen, for example, in the implementation of formalized processes. For example, they help structure risk management so that activities are not overlooked and enable the benchmarking and certification of standardized approaches (von Solms 2000). Although formalized processes can be viewed as dead, they contain some traces of "*previous lives*" (D'Adderio 2011, p. 207) in the sense that they consist of

codified compilations of combined experiences and practices (von Solms 2000). Dead routines can therefore be seen as the glue that holds the patterns of risk management activities together, thereby playing an important role in laying out a path for human actions to take place (D'Adderio 2011) and guiding them away from being performed ad hoc (Parnas and Clements 1986). The notion of dead routines has, however, been criticized in the risk management literature for often omitting individual and social aspects (Ashenden 2008; Coles-Kemp 2009) and for assuming the predictive capacities of its practitioners (Njenga and Brown 2010, 2012).

Alive routines can be described as recognized, emerging patterns of activities that are enacted by multiple, reflective, and knowledgeable practitioners (D'Adderio 2011; Feldman et al. 2016; Pentland and Feldman 2008). Activities performed as alive routines can therefore vary as practitioners reflect, gain new insights, and accumulate new experiences. Variations in performance and adaptations to activities may be introduced because "*easier, more effective, more fun, more familiar, or more attractive or aesthetically pleasing*" ways are found by the practitioners (Feldman et al. 2016, p. 508). Alive routines can, as such, be seen as an emergent accomplishment, continuously shaped as practitioners interpret and make sense of real situations and adapt their actions accordingly. The sequence in which activities are performed is therefore often meaningful and contains insights into what brings about variations and adaptations (Feldman et al. 2016).

3 Research Approach

3.1 Research Environment

This research has been conducted in close relation with public sector organizations and government agencies in Sweden. There are three reasons for this. First, the ability of the public to access official records made internal policies of public organizations more accessible. Second, the organizations that were investigated provide services and data that are critical to society. Risk management is therefore an important aspect of the organizations studied, as the disruption or destruction of these organizations' information systems could, for example, affect national capabilities to emergency responses. Third, public sector organizations and government agencies in Sweden are required to systematically conduct risk management—which is further mandated by external requirements such as the EU's general data protection regulation and the network and information security directive. Nevertheless, there is no enforced formalized process to abide by. This has led to an access to study different practices, simultaneously providing an environment in which it has been possible to interact with practitioners, to investigate their approaches to and their different formalized processes of risk management, and to explore their reasoning for utilizing the approaches and method as they do.

3.2 Research Methodology

This study has followed an explorative, qualitative research approach. The data that have been collected come mainly from interviews, document analysis, and observations and have been analysed using a text analysis method. Considering the research purpose, the qualitative approach was selected because it provides an opportunity to study organizational behaviour and practices in richer detail, thus providing insight and understanding that would have otherwise not been accessible by adopting a quantitative approach (Marshall 1996). This is not to say that a qualitative approach comes without limitations. For example, the findings cannot easily be generalized.

A quantitative research method, such as a survey study, could gather data about which risk management practices are used in organizations, for example. While such an approach could lead to valuable insights, it cannot capture the practitioners' experiences and reflections about how those practices are enacted or why they are implemented. Thus, a quantitative approach would describe the general, but not cover the particular (Hyde 2000). Therefore, an explorative, qualitative approach was selected as it is able to support the attainment of empirical insights into the studied phenomena.

3.3 Data Collection

Data for this research were collected from public sector organizations and government agencies in Sweden through interviews, document analysis, and

observations. Reasoning about implemented processes and their enactment were presented and discussed with an expert panel as a validation session. Data were also captured through observation. The interpreted information was brought back to the respondents to ensure that it was accurate to their own experiences (Silverman 2015).

It should be noted that rich insights can be found from studying particular interest in a chosen and limited area (Kvale 1996; Patton 2014). Saturation of the chosen topic, patterns, and recurring themes are all measures of whether additional data collection is needed (Mason 2002). Table 1 below presents an overview of the studies in which the data have been collected.

Table 1 – Overview of data in relation to studies.

Part of Study	Type of Data
Paper A	Literature review targeting seven different journals, resulting in 73 articles collected; 27 of these articles were relevant, included, and analysed in the study.
Paper B	Empirical study including interviews carried out in four different government agencies and one pilot interview. In addition, internal guidelines and standards were collected from each respective organization.
Paper C	Empirical study including interviews carried out in four different government agencies and one validation session of the findings. In addition, internal policy documents were collected from each respective organization.
Paper D	Empirical study including observations carried out in two different public sector organizations. This study included two group interviews, one joint group interview, and one validation session of the findings. In addition, internal documents outlining the organizations' internal risk management documentation were collected.

3.3.1 Literature review

The literature review was adopted as the first conceptual study to analyse and synthesize literature related to practical aspects of risk management capabilities. Using Ritchie and Spencer's (2002) framework of analysis, and Okoli and Schabram's (2010) steps for conducting a systematic literature review, a predefined search protocol was established. The search protocol included a plan for how the review process should proceed and consisted of a search strategy, a practical screening, a quality appraisal, and data extraction and synthesis.

The search strategy focused on journals within the field of information systems and used the following search phrases to identify relevant articles: "information security" AND ("risk management" OR "risk practice" OR "risk mitigation" OR "risk assessment"). This search resulted in 73 articles that were available for practical screening. Articles that reflected on abilities to adapt, integrate and reconfigure skills, resources and competencies to achieve various risk management-related activities were included for data extraction and synthesis. This resulted in 27 relevant articles retained from the

original 73 for further analysis and extraction. The data extraction and synthesis method followed this process, consisting of five steps as proposed by Ritchie and Spencer (2002). This process consisted of (1) familiarization, (2) identifying a thematic framework, (3) indexing, (4) charting, and (5) mapping and interpreting. Extracted data were mapped into a concept matrix, further synthesized, and analysed into themes.

3.3.2 Secondary data collection

Internal risk management guidelines and standards of the public sector organizations and government agencies that were used for this study, as well as established standards, e.g., ISO/IEC 27005 (2018) and NIST SP 800-30 (2012), were analysed. This provided a theoretical backbone, as the organizations' formal processes supplied important background information into how such processes are intended to work. The analysis further provided an understanding of what of rules and expectations the formal processes suggested. Apart from providing richer insight into the practices, the internal guidelines and standards that were collected also provided input to the interview guide needed for the follow-up interviews, as described below.

3.3.3 Semi-structured interviews

Semi-structured interviews characterized by open-ended questions were used to collect data directly from respondents (Longhurst 2003). An interview guide was prepared beforehand and used during the interviews. The guide consisted of thematic questions and scenarios. The interviews were recorded. Notes were taken not only to help capture ideas and impressions but also to help interviewers encourage elaboration of topics and to assist in going back to certain points of interest during the interview. The interviews were conducted with one researcher asking questions and another taking notes as well as following up by asking additional questions if something needed clarification or further elaboration. The interviews started by explaining the focus of the study, followed by the researchers asking for permission to record the interview. Similarly, to make the respondents feel free to speak freely, the material was anonymized.

3.3.4 Observations

Observations were carried out in a series of workshops within two public sector organizations which had a novice-level understanding and implementation of security. A university-level commissioned risk management educator, currently educating public sector risk management practitioners, was contacted to get in touch with the novice risk management practitioners willing to participate in the study. Each workshop covered a particular topic, for example, asset identification or risk analysis.

Throughout the observation, the researchers acted as complete observers, meaning that they took no part in the workshops (Oates 2005). The conversations from the workshops were recorded, but video recording was not possible. The observations were followed up by interviews with the participants from the respective organizations, both in separate group interviews and in a joint group interview. That is, a group interview was conducted directly after each observation and a joint group interview with participants from both organizations was also conducted. The interviews were conducted to ask clarifying questions, for example, about documentation practices, and more reflective questions about the learning that was taking place in the workshop.

3.4 Analytical Perspective

Considering the different formalized processes, there are some challenges to investigating risk management as parts of a process since activities are often described differently. However, although various processes differ in their individual parts, an abstraction has been made based on some of their shared common goals. A set of common risk management activities that are not biased towards any particular formalized process has been defined based on such goals, i.e., identification of assets, analysis of risks, and treatment of risks. The use of an established and more comprehensive process, such as NIST SP 800-30 (2012) or ISO/IEC 27005 (2018), as a frame of reference, was found to place more focus on the process itself. In contrast, this set of common risk management activities was found to be more inclusive and was used to categorize risk management activities as discussed by the respondents. Thus, a series of descriptions detailing what was excluded or added in relation to a particular process could be avoided.

Practice, which, according to Schatzki (2012) and Cox (2012), can be defined as a set of organized human activities, or doings, linked by shared understandings and instructions, has provided an analytical lens. Understanding refers to how a desired action is to be carried out, whereas instructions refer to formulated rules or directives outlining what to carry out (Schatzki 2012). Similarly, an activity is a practice if the action of engaging in that activity gives meaning to it and is consequential for its existence and development (Feldman and Orlikowski 2011). That is, practice is about doing, and the meaning of practice is socially constructed through the expected outcome of engaging in it and knowing how to do so.

This type of perspective offers an analytical concept that enables interpretation of the way in which people achieve activities, and of how practices become socially recognized as ways to perform a particular activity (Gherardi 2009).

3.5 Data Analysis

The recorded material from the interviews and observations was first transcribed, and the notes were aggregated (Schmidt 2004). The analyses focused on capturing the reasoning in practice, highlighting the enactment of activities by the respondents.

The analysis followed concept-driven coding to categorize the transcribed data. This was done in four steps. First, each researcher individually read through the material, and they highlighted relevant excerpts in the transcript and noted these down along with key concepts, suggestions for codes, and motivations for inclusion. Second, the highlighted text from the transcripts was joined, sorted, and grouped according to the suggested codes. Third, the researchers jointly examined each suggested code, its extracted transcript text and its key concepts. Fourth, after discussions, each key concept was synthesized into a coherent text under the agreed upon set of codes. Differences between researchers were resolved by discussing and examining the motivations for inclusion and the suggested codes.

3.6 Overview of Papers

The initial research was based on a literature study, which aimed to establish the organizational risk management capabilities that could be found in the literature. The purpose was to understand the underlying intentions and knowledge required to

conduct risk management, as presented in previous studies. The literature review resulted in eight capabilities (Letter A, Figure 1), which were seen as potential challenges for organizations conducting risk management. Using the identified challenges as a perspective, the subsequent study focused on whether those challenges had implications for risk management in practice—and if so, how. Interviews were thus conducted with four different government agencies. The interview questions were derived from the identified challenges. The findings indicated a tension between dead and alive routines—i.e., guidelines and actual performance—which affected how the formalized processes were carried out (Letter B, Figure 1). Figure 1 below shows an overview of the enclosed papers and their findings.

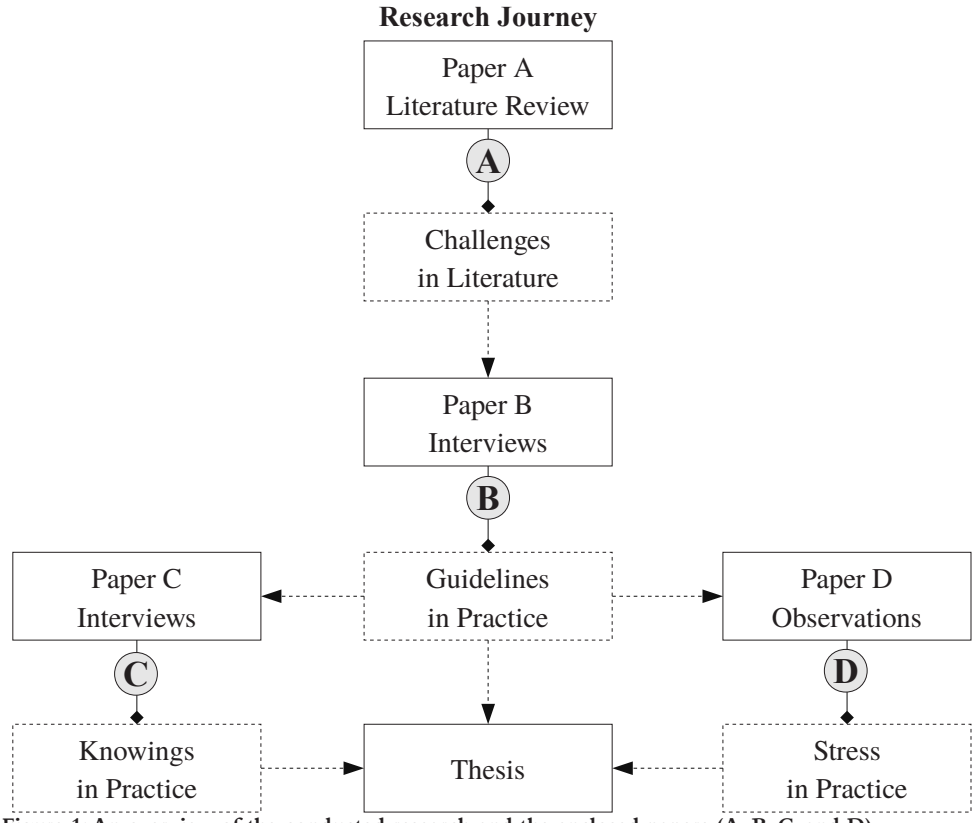


Figure 1: An overview of the conducted research and the enclosed papers (A, B, C, and D)

To further understand how risk management is performed in practice, four challenges as identified by Fenz et al. (2014) were analysed. Drawing from the findings of Paper B, the focus in Paper C was on understanding what practical insights and reasoning could be found in overcoming the challenges, suggested by Fenz et al. (2014). The resulting study was based on interviews with four different government agencies and resulted in a series of knowings—i.e., themes of actions carried out to overcome some practical difficulty and to keep risk management alive (Letter C, Figure 1). Up to this point, the studies that had been conducted had focused on organizations with a history of previous

risk management experience but also reflected on the challenges faced by security-novice practitioners. This led to the next study to determine whether—and if so, how—security-novice practitioners, when faced with the challenge of implementing and conducting risk management activities within their respective organizations, were influenced in their security decisions. The study involved two different public sector organizations and confirmed a tension between dead and alive routines that caused stress for the security-novice practitioners and influenced the decisions that they made in practice (Letter D, Figure 1).

4 Summary of Appended Papers

4.1 Paper A

Lundgren, M. (2020) 'Rethinking capabilities in information security risk management: a systematic literature review,' *Int. J. Risk Assessment and Management*, Vol. 23, No. 2, pp.169–190.

4.1.1 Summary

In Paper A, the concept of capabilities within risk management was investigated. While previous research has made important contributions to risk management, there is an incomplete understanding of the underlying capabilities necessary to perform its activities in the literature. Studying capabilities embedded in routine work could, however, give insight into what enable people to practice risk management, such as their underlying know-how and intentions.

A theoretical framework was therefore proposed in which capability is distinguished by 'knowing' and 'intent,' and is defined as an on-going accomplishment that is constructed and reconstructed as practitioners engage in risk management activities. In this framework, 'knowing' refers to the ability to define, prepare, shape, and learn to solve a task or a challenge and 'intent' as the desired future outcome that shape the practice in the present. As such, capability constitutes the alignment between the 'intent to do' and 'knowing how to do.' The suggested framework is an effort to further this explanation and to propose a foundation for a common perspective on capabilities.

Using the framework combined with a set of general risk management activities, capabilities were identified by collecting and analysing information security literature. As a result, eight capabilities in total were identified that affected each risk management activity in terms of the identified intent and knowing. The study concludes, however, that capabilities can be associated with intent and knowing on a conceptual level but not in an instrumental sense. Capabilities are, for example, not something that an organization has but something that can be achieved as people engage in tasks and challenges. In other words, the capabilities identified in this study did not define actions to take and follow but rather identified what enabled or constrained a particular activity. In this regard, each of the eight identified capabilities could become challenges if not managed accordingly.

4.1.2 Relation to thesis

This study highlights the tension between the intent to do something and knowing how to do it. Hence, it tries to encapsulate and point to the importance of the practical know-how necessary to carry out different activities and the role that meaning has on actions. In short, what enables people to perform risk management.

4.1.3 Division of work between authors

As the sole author, I did all the work myself.

4.2 Paper B

Lundgren, M. and Bergström, E. (2019) 'Dynamic interplay in the information security risk management process,' *Int. J. Risk Assessment and Management*, Vol. 22, No. 2, pp.212–230.

4.2.1 Summary

In this paper, the effect of social and organizational challenges on risk management in practice were studied. Risk management in this context was depicted and described as a predominantly instrumental process. To this end, such descriptions serve as rational guidance in terms of the implementation of a sound process.

Considering that actual processes are shaped within the enactment of day-to-day activities and their respective challenges, a rational process gives rise to the perception that these activities are not dynamic, but static. Because of this, the rational description of the process may be overvalued while simultaneously the situated enactment, i.e., how practice adapts its processes to real situations, is undervalued. In Paper B, it was proposed that risk management processes are not static but that there is a dynamic interplay between activities that shape and affect each other as a consequence of organizational and social challenges that 'lie between' each activity. It was proposed that by investigating this dynamic, clues could be found about how the enactment of risk management activities adapts to a particular context and shapes its process within the context.

To investigate this matter, Paper B targeted four major Swedish government agencies using the eight capabilities identified in Paper A—but here they were framed as challenges instead—as the basis for interview questions. The interview questions focused on the agencies' risk management activities, their day-to-day practices, and their formalized processes to gain insight into underlying motivations and reasoning.

As a result, twelve characteristics of both social and organizational natures were identified that illustrated an interplay between different risk management activities. It was found that, contrary to what rational descriptions of formalized processes suggest, different risk management activities were performed in an order that, at the time, made the most sense. This was influenced by organizational factors, such as budget or use of technology, which could motivate altering an activity's outcome. However, socially constructed concepts, such as asset value or held beliefs, could justify omitting a particular risk management activity altogether. This led to deviations from what had otherwise been described as a guiding process.

4.2.2 Relation to thesis

This paper reports on the dynamics between instructions and actual practice. In particular, it illustrates an interplay between normativity and meaning of practice and how this affects the process. It was also indicated that the process was not static but emergent, as a result of the tasks that the practitioners had to solve.

4.2.3 Division of work between authors

In this paper, the study design, planning, data collection and analysis were performed together with the second author. Since this paper built heavily upon the findings from Paper A as a foundation for the data collection, I authored most of the introduction, problem description, and theoretical background myself.

4.3 Paper C

Bergström, E., **Lundgren, M.**, and Ericson, Å. (2019) 'Revisiting information security risk management challenges: a practice perspective,' *Information & Computer Security*, Vol. 27, Issue: 3, pp.358–372.

4.3.1 Summary

It is commonly agreed that a successful implementation of a risk management process for information security is one that aligns well with other organizational objectives. However, research within the area has long suffered from relatively few empirical studies, and there is little advice on how to achieve such alignment in practice. The lack of empirical studies has made it difficult for researchers and practitioners alike to draw insights into how organizations work. As a consequence, little is still known about what challenges organizations are confronted with in their activities and how they meet those challenges.

Therefore, this research stream was furthered by empirically exploring challenges that were grounded in the organizational management of risks. Building on and refining six previously identified challenges within risk management, Paper C studied the reflective actions that were taken by four Swedish government agencies to overcome such challenges. These reflective actions, here called 'knowings,' were routine actions taken to get the work done.

As a result, four knowings were identified that in some way affected how the continual social construct of experiences was applied and formed in day-to-day risk management work. The identified knowings were formulated as knowing to be 'good enough,' knowing to 'hurry slowly,' knowing that 'there is no silver bullet,' and knowing the 'bigger picture.' The practical results of applying these knowings illustrated how the actual content of risk management activities was not created by the espoused instruction found in the respective agency's formalized process but had evolved in practice based on what made sense to the practitioners. Examples of this included instances where shortcuts in the process had been developed to remove ambiguity or where the internal language used in the process had been homogenized to avoid misunderstandings.

4.3.2 Relation to thesis

The content within management processes was shown not to have been created by the espoused instructions found in formalized processes. In its place, the employees formed their own shared interpretation and experiences. This paper highlights this conclusion by pointing towards the observed value of building and maintaining a culture of learning, which recognizes that there is no one method that fits all situations. Instead, actual work routines emerge over time as activities form and adapt to specific contexts. Learning could thus be recognized as an ongoing accomplishment that is constructed and reconstructed as practitioners engage in practice.

4.3.3 Division of work between authors

The main idea behind the paper was mine, where I sat the focus of the paper, and authored most of the introduction and problem description myself. The research planning, data collection and analysis was done by the co-author and me.

4.4 Paper D

Bergström, E., **Lundgren, M.** (2019) 'Stress Amongst Novice Information Security Risk Management Practitioners,' *Int. Journal on Cyber Situational Awareness*, Vol. 4, No. 1, pp.128–154.

4.4.1 Summary

Paper D furthers the research and concept of security-related stress (SRS), as first introduced by D'Arcy et al. (2014), by applying it to risk management. SRS refers to demands on one's cognitive resources or abilities caused by internal or external security-related requirements and demands, which are experienced by the individual as burdensome, complex, or ambiguous. In particular, SRS refers to three dimensions of stress: overload, complexity, and uncertainty. A security-novice employee is likely to experience burdensome, complex, and ambiguous security requirements. Thus, they also experience SRS, which influences their security decisions (D'Arcy et al. 2014).

As security concerns grow, new laws and regulations are passed that require security to be managed. However, many organizations lack personnel with the necessary experience required to manage and adapt risk management processes to their specific practice. Considering that many formalized processes have been shown to require a great amount of expertise to apply, we set forth that risk management may be improved by studying novices to risk management.

The study targeted two organizations that were in the early phases of developing and implementing risk management processes but that had limited or no previous experience related to the task. By using a case study approach to obtain data about their practices and using SRS as a perspective, the study found indicators of SRS that, in some way, affected the two organizations' respective processes. SRS was analysed from its three dimensions, where each dimension included stressors—i.e., factors that create stress—as well as stress inhibitors—i.e., factors that decrease stress. It was found that there was a mismatch in how formalized processes were conceived and how they were interpreted in practice. The mismatch created stress as it either led to an overload of work, a feeling of inadequacy with regard to skills, or a need to stop and investigate various security-related matters (complexity) or requirements of new processes calling for a change in established work routines (uncertainty).

4.4.2 Relation to thesis

The study not only introduces, but also builds upon the observed 'tension' between dead and alive routines. During the study, this tension resulted in stress and highlighted indicators of SRS. The study thus contributes to the understanding of the complexity involved when transforming formalized processes into actual practice.

4.4.3 Division of work between authors

The main idea behind the paper was mine, where I sat the focus and theoretical positioning of the paper, and authored the abstract, most of the introduction, and problem description myself. The validation data were collected by the co-author.

5 Dynamic Routines

5.1 Between Controlling and Shaping

The formalized processes entail control and guidance of actions that instruct organizational activities for practitioners to follow and act upon—i.e., if they are interpreted instrumentally, they will result in dead routines. As such, formalized processes influence the strategy for how to go about carrying out the instructed activities and the actual performance in practice. This is illustrated in Figure 2 by unidirectional arrows; Letter A affecting strategy, and B affecting performance. Accordingly, in this view, formalized processes become, if left by themselves, settled—i.e., dead.

Alive routines entail a continuously shaping process between strategy—i.e., how the activity is planned—and performance—i.e., how the activity is actually carried out. The strategy for how to carry out activities is therefore shaped and re-shaped over time as new experiences are gained from practice. In this sense, strategy enables practitioners to account for and to formulate how to perform particular activities—thus creating understanding (Letter C, Figure 2)—which can either constrain or assist the activities. There is therefore an interplay between strategy and performance that enables practitioners to understand how to perform activities and supports them in doing so in practice. Experience (Letter D, Figure 2) is gained through doings in practice and leads to new insights and inspiration that influences future strategies for how to perform those same, or similar, activities. It should be noted, however, that gaining understanding and experience from practice comes from achieving both successful and unsuccessful results.

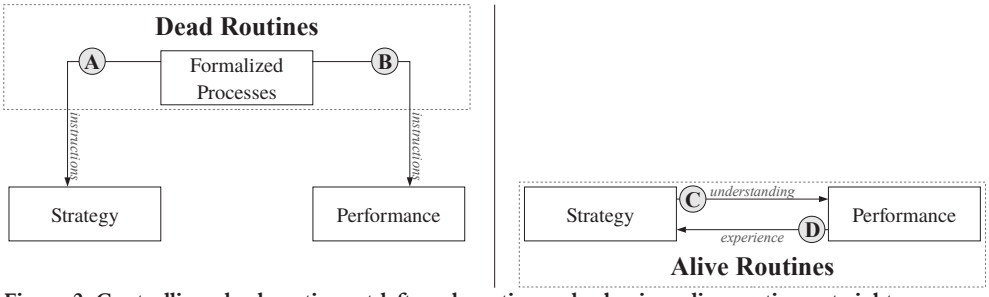


Figure 2: Controlling, dead routines at left, and continuously shaping, alive routines, at right.

However, without supportive, formalized processes, there is a danger that risk management could become too developmental. Two additional relationships can be discussed in relation to formalized processes, namely, rationale (Letter E, Figure 3), and implementation (Letter F, Figure 3). That is, while formalized processes provide instructions for what to do, the chosen strategy reflects the practitioners' rationale based on those instructions—e.g., interpretation, meaning, or relevance. A match between instructions and rationale indicates that formalized processes are readily understood and

accepted, whereas a mismatch gives rise to variations, divergences, or alterations of the prescribed formal process. Implementation reflects the practitioners' realization of formalized processes. A match between instructions and implementation indicates control, in the sense that the formalized processes are complementing the practice and are applied as intended, whereas a mismatch gives the practitioners indications of a need for adaptations and for reconsidering how activities should be performed.

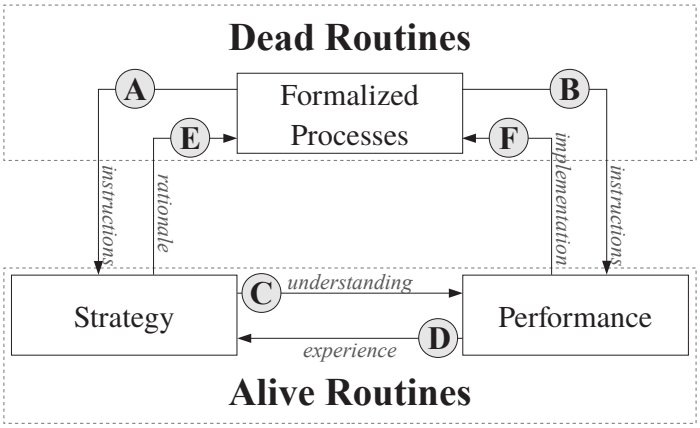


Figure 3: The dynamic between controlling and shaping, i.e., what makes dead routines alive.

This model, as a whole, provides insights into risk management, by explaining how and why the interplay between controlling and shaping do—or do not—appear in practice.

5.2 Empirical Insights

The empirical results will be analysed and discussed from three types of risk management activities that have been in focus for the data analysis, namely:

- '**Asset identification**,' which refers to risk management activities that aim to establish what assets to protect. This includes identifying, classifying, and valuating information assets, regardless of their form, be it tangible or intangible. The result of this activity typically serves as input for the next activity, risk analysis, to inform what to protect and the level of protection that it requires.
- '**Risk analysis**,' which refers to risk management activities that aim to define, identify, and evaluate risks. This includes threat and vulnerability identification, evaluation, and prioritization, which help in the selection of possible security controls. The result of this activity typically serves as input for the next activity, risk treatment, to inform how to protect the identified assets based on the assessed risks.
- '**Risk treatment**,' which refers to risk management activities that aim to select treatment strategies and implement related security controls. The outcome of this activity typically results in one or more administrative, technical, managerial, or legal implementations or changes to modify the identified security risks to an acceptable level. The process can then start over again, as needed.

5.2.1 Asset identification

Two respondents from two different government agencies, along with a third respondent from a public sector organization, described asset identification as a separate and isolated activity to be performed before risk analysis. They added that it is difficult to avoid reflecting on risks while conducting the activity (Paper B). This can be interpreted as these respondents perceiving a mismatch between the instructions and the strategy for performing the activity, although each organization's formalized process describes asset identification as being performed separate from the risk analysis. The formalized process in one of the respondents' organizations noted that during asset identification:

> "*risks should not be taken into account, but the focus should be on the consequences towards the organization.*"
>
> – Formal process in a government agency

Similarly, another respondents formalized process also described the following:

> "*asset identification can be performed as needed to help clarify requirements* [...] *before a risk analysis.*"
>
> – Formal process in a government agency

One of the respondents explained that risks are sometimes used in asset identification to elaborate on what could happen to the asset and thereby help determine its value. With a tone of regret that implied it was wrong to discuss probabilities of risks during asset identification, the respondent continued to explain that risk, and asset identification are two separate things that should not be mixed:

> *"When we do* [asset identification]*, people easily say, 'This will not happen'. However, then you have to intervene and say, 'Hold on, we are supposed to only consider consequences, not probabilities… these* [activities] *are separate things."*
>
> – Information Security Coordinator (Paper B)

A similar approach was observed during a workshop among security-novice respondents (Paper D). As the respondents engaged in the asset identification activity, one of the respondents notified that the discussion drifted into the topic of risks. When this happened, the respondent declared that they were getting ahead of themselves and turned the conversation back to the actions associated with asset identification. In effect, the respondents discarded the risks they had just identified since:

> *"*[The risks] *will be shown later in the risk analysis."*
>
> – Information Security Coordinator (Paper D)

In a follow-up interview, the respondent commented on risk and asset identification, saying that:

> *"it comes as a natural step to think about risks during the* [asset] *valuation."*
>
> – Information Security Coordinator (Paper D)

One possible reason as to why they had let the formalized process control the activity, despite it being perceived as not purposeful, was provided during the joint group interview:

> "*it is difficult to admit that maybe we didn't follow the routines, especially if the boss is present in the meeting, and that maybe we are a bit uncertain* [about the risk management process]"
>
> – Information Security Coordinator (Paper D)

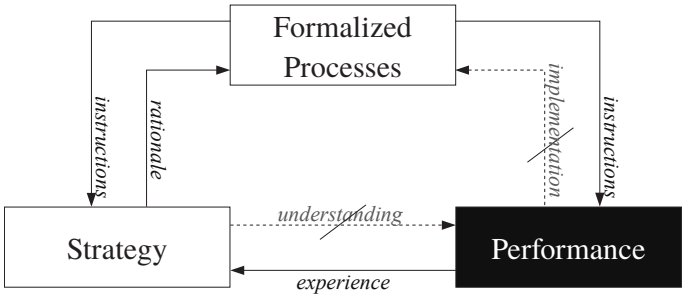


Figure 4: A mismatch between the formalized process and strategy.

In these empirical observations, the formalized process restrained the strategy since the respondents perceived that they had deviated from the instructions. That is, they found a mismatch between how they were supposed to do and what they found was meaningful to do to find a more accurate asset value (Figure 4, upper left). However, the controlling characteristic of the formalized process was adhered to over the practical approach favoured among the respondents. In parallel, the respondents perceived a mismatch between the instructions and their implementation, but they conformed their performance to the instructions, thus, hampering potential improvements to the formalized process (Figure 4, upper right). The strategy for how to perform the activity therefore remains based on instructions, rather than based on the experience gained from introducing risk reflections into the asset identification. It can, in this case, be argued that the formalized process did guide the risk management activities; simultaneously, the respondents did not suggest adaptations due to being unsure of whether or not such suggestions would be appreciated by "*the boss.*" This resulted in a change of strategy, in which the asset identification and risk reflections were separated, despite being found as a meaningful performance (Figure 4, bottom).

5.2.2 Risk analysis

One respondent described how the instructions in their formalized process on risk analysis had changed over the years. These changes were made to make the process more resource efficient (Paper C). The respondents further explained that they had previously carried out risk analysis with the help of an algorithm to calculate and prioritize risks to decide which final security controls to implement. However, it was found that nobody used the algorithm, and the risk analysis often resulted in the same, or similar risks each time the activity was performed:

> *"I know that perhaps 33 of the same risks will show up in different applications* […], *so I would already know the answer when I do this the third time or so* […]. *We used to have a small algorithm before that helped put a value on different security controls,* […] *but I removed it after having spoken with other managers and having asked if they used it, and they all said no."*
>
> – Security Specialist (Paper C)

The respondent explained further that rather than using risk analysis to help decide on security controls for the risk treatment activity, a predetermined list of security controls was now used that correlates with particular asset types. However, the respondent also drew attention to the potential downside of not performing a unique risk analysis each time the activity was performed. Namely, using a predefined list of security controls would overlook unidentified risks. Nevertheless, the perceived increased efficiency outweighed that potential downside:

> "[We] *miss maybe 5 percent of risks that are never found, and the only way to find them is to make a unique risk* [analysis] […] *Our way of doing it still covers most of the risks, and it provides much better use of resources."*
>
> – Security Specialist (Paper C)

The quick approach, namely, to directly associate asset types with particular security controls, was shown to make more sense for the respondents than carrying out a lengthy risk analysis and provided a more consistent approach for identifying and implementing security controls. Additional respondents also described the risk analysis activity as too complex and time consuming and therefore as something that made little sense to conduct on a regular basis. Another attempt that an organization had made to speed up the risk analysis was described by a respondent. This respondent noted that because they kept finding the same or similar risks each time a risk analysis was performed, they had stopped performing risk analysis on individual assets, such as single IT units. Instead, risk analysis was mainly performed on larger systems, such as business systems, if they suspected that there might be something out of the ordinary threatening that system:

> *"So, we have determined that… risk analyses are primarily done for infrastructure systems, eh… the business systems* […] *if we can see any risks that are out of the ordinary, such as clear deviations from normal operations* […], *but that puts a lot on my colleagues, having that knowledge about our systems and how they work* […]; *so, it becomes sort of a reduced risk analysis."*
>
> – Security Architecture (Paper C)

The strategy for carrying out the risk analysis is shaped here by relating it to earlier performances, e.g., the required time, resources, and complexity (Figure 5, upper right). The shortcomings that were experienced involving the performance of a unique risk analysis each time led the respondents to not follow the instructions, but rather to follow their experiences that inspired future strategies for how to alter the activity (Figure 5, bottom). This understanding was further introduced as a new part of the formalized process and thus improved the instructions accordingly (Figure 5, upper left).

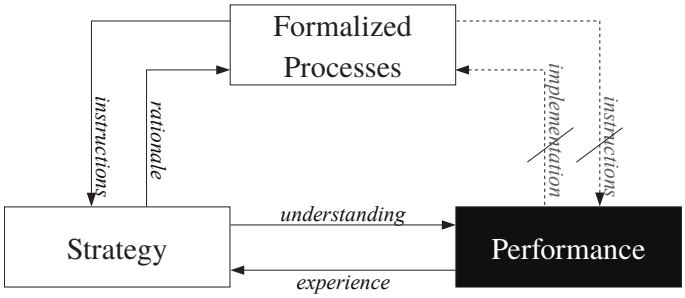


Figure 5: An adaptation created from performance.

A similar approach was found among the security-novice respondents, one of which described the situation and highlighted the quantity of resources that it took to perform the risk analysis:

> *"We cannot have a situation where our organization gets affected by us sitting and doing risk analyses all the time."*
>
> – Information Security Coordinator (Paper D)

Other respondents explained similar problems and discussed how to solve them. One suggestion was to:

> *"connect information value to security controls…* [since it] *maximizes* [time utilisation]*."*
>
> – Information Security Coordinator (Paper D)

Thus, the respondents described similar experiences from performing risk analysis, e.g., that it was time and resource consuming. However, instead of letting the experience shape an alternative strategy, since this one was found to be unproductive, the respondents followed as best they could the instructions as described by the formalized process (Figure 6, bottom). In this case, the experiences from performance did not shape an alternative strategy (Figure 6, upper left). Instead, the activity was implemented in accordance with the established process (Figure 6, upper right).

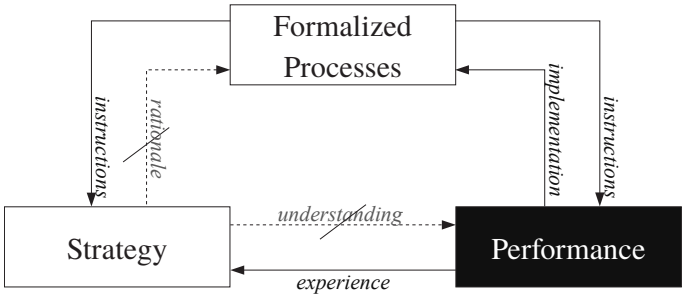


Figure 6: A situation which did not alter the formalized process.

5.2.3 Risk treatment

Respondents described that the final security controls are not always selected based on the initial result from the risk analysis but are modified based on cost or complexity. This contrasted the different organizations' respective formalized processes, which described risk analysis as motivating security controls. One formalized process noted that security controls should be:

> "*Based on the company's risk analysis, system security analysis, and its incidents.*"
>
> – Formal process in a government agency

It was mentioned by the respondents that sometimes, however, security controls have been suggested in the risk analysis that are either too complex or too costly to implement. One respondent explained that when the risk analysis activity is completed, and the risk treatment begins, it is discovered that the security controls motivated by the risk analysis are unfeasible:

> *"But then we find that we don't have the technology to live up to the* [security controls] *that we actually wanted to implement, and that the cost to implement them would be too high, so we have to settle for a cheaper alternative."*
>
> – Information Security Coordinator (Paper C)

In this case, the respondent described how they had to adapt the result of the initial risk analysis to find a less costly alternative. Another respondent, similarly, noted that in this situation:

> *"One would only need to go back one step* [to the risk analysis]*: are there any other security controls that could provide a similar result but are not as costly?"*
>
> – Director of Preparedness and Response (Paper B)

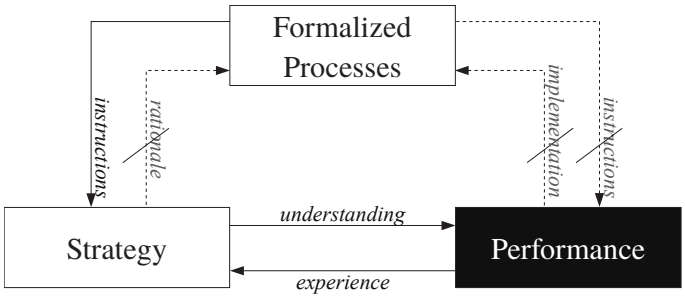


Figure 7: A mismatch between formalized process and performance.

These empirical observations illustrate a mismatch between the formalized process and the performance, i.e., how the activity was actually carried out (Figure 7, upper right). In this case, the proposed security controls were not acted upon because they were determined to be too complex or expensive. Instead, the output of the risk analysis was adapted to fit expectations based on insights gained from performing the risk

treatment activity (Figure 7, bottom). However, this case also points towards a mismatch between how the instructions, or lack thereof, are translated into a strategy (Figure 7, upper left).

In one of the organizations, the formalized process does not take cost into account for the risk analysis, which may explain why it could become an issue during the risk treatment. However, the dimension of cost is partly addressed within the formalized process in one of the organizations, but only as a recommendation to be considered:

> "*IT specialists can be included in the discussion to describe costs that can result from suggested security controls.*"
>
> – Formal process in a government agency

One respondent stated that the instructions were there, simultaneously explaining the challenges of turning the instructions into practice:

> *"The policy for assigning asset values are clear and easy to follow,* […] *but I think that there is still something missing, some parameter for reaching a decision on countermeasures in terms of time and money."*
>
> – Information Security Coordinator (Paper C)

Insights gained from performing the risk treatment activity can therefore not only inform the risk analysis about changes to proposed security controls, but can also inform the risk analysis about the inclusion of additional ones. One respondent explained that the security controls proposed in the risk analysis were sometimes found to be insufficient during the risk treatment, and that new security controls are then created as a complement:

> *"Sometimes we say in the risk analysis, 'Yes, this* [risk] *is manageable,' but then as we start with the security control step, we see that we won't be able to manage the risk fully with the technological security controls, and perhaps we have to create a manual routine on the side* […] *as a complement."*
>
> – Security Specialist (Paper C)

Variations in the performance of the formalized process occurred to adjust the results of the risk analysis to fit the particular organizational context. Insights gained—such as obstacles like cost or complexity of security controls—from one activity can shape the strategy for how to perform another; here, the risk treatment informed the risk analysis.

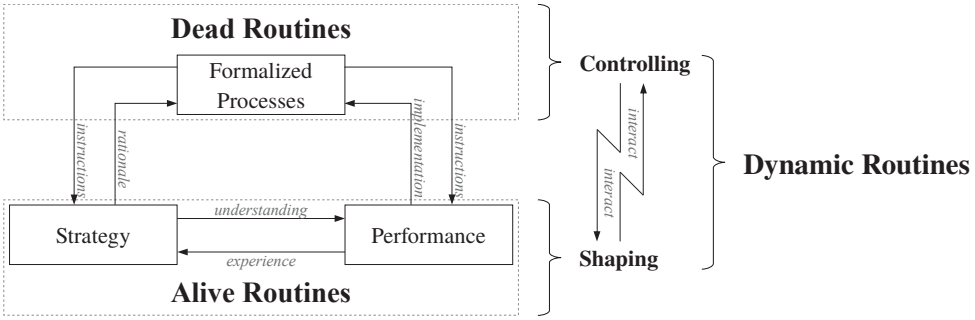


Figure 8: Dynamic routines as the interplay between dead and alive routines.

In final remarks, dead routines prescribe instructions that are based in theory and can serve as controllers for practitioners' alive routines, which are otherwise shaped freely over time by experiences and understandings as gained from practice. It is, however, within the interaction between controlling—i.e., formalized processes—and shaping—i.e., the interplay between strategy and performance—that flexible and emergent processes of adaptations arise, which can be described as a dynamic routine (Figure 8). In other words, it is when dead and alive routines interact and influence one another that these dynamic routines occur. Dynamic routines are therefore useful, as they appear in response to mismatches that are experienced between formalized processes, strategies, and performance, to, for example, adjust activities to better fit expectations or to overcome obstacles found in practice.

6 Conclusions

The purpose of this thesis has been to examine how and why adaptations occur in risk management. This was done to contribute to a better understanding of how practitioners take action in practice to meet challenges and new circumstances. This explorative study has been closely related to public sector organizations and government agencies in Sweden. An explanation model has been used to elaborate on dynamic routines that arise in the interaction between the practitioners' controlling and shaping of activities. Controlling is here defined as codified instructions prescribed in formalized processes, and shaping is here defined as emergent patterns of activities based on performance. In cases where the formalized process is applied directly to an activity, risk management becomes instrumental, but is not improved to fit new circumstances. However, time and resources can be saved by adapting the instructions in some cases. In cases where the performance reshapes the formalized processes and, in turn, reshapes the strategy, risk management gives rise to dynamic routines. These appear:

- When a mismatch between the formalized process and the practitioners' experience, understanding, implementation, and rationale occur.
- In response to complexity, as a means of simplifying or speeding up a particular activity, such as having a direct correlation between security controls and asset types.
- As an interplay between activities to adjust outputs to fit expectations, such as cost or level of complexity in security controls.

6.1 Practical and Theoretical Implications

The practical implications are mainly the awareness and opportunities available from recognizing how and why dynamic routines appear. Overvaluing the formalized process and thereby undervaluing situated practice and sense making may cause less engagement among practitioners by discouraging creativity in problem solving.

Therefore, the alive routines of risk management benefit from being continually reflected upon in the instructions prescribed in formal processes. This could be done by encouraging that adjustments be added over time as insights and that examples be obtained from practice. Thus, making the practitioners the owners of the emergent formalized process, rather than simply the implementers. By taking advantage of reflections made in activities, others can add to and learn from them. Dialogues, e.g., new ideas, questions, or difficulties could help capture such reflections but also could create awareness that risk management is not a precise—dead—routine but a craft, something that is alive and adjusts over time.

6.2 Future Research

Since these studies have addressed governmental agencies and open public organizations, I would like to suggest future studies focused on other types of organizations. Considering that these organizations are, in Sweden, mandated to work systematically with information security, they could have different prerequisites, attitudes, or time and resource constraints than other types of organizations would. Additionally, international studies are recommended to be explored in the future, since different organizational cultures probably play a role in risk management. Furthermore, an increased focus on the role of the practitioners is suggested, since practitioners might associate risk management with how they perceive their occupation or professional identity.

References

Al-Ahmad, W., and Mohammad, B. 2013. "Addressing Information Security Risks by Adopting Standards," *International Journal of Information Security Science* (2:2), pp. 28–43.

Amraoui, S., Elmaallam, M., Bensaid, H., and Kriouile, A. 2019. "Information Systems Risk Management: Litterature Review," *Computer and Information Science* (12:3).

Ashenden, D. 2008. "Information Security Management: A Human Challenge?," *Information Security Technical Report* (13:4), pp. 195–201.

Baskerville, R., Rowe, F., and Wolff, F.-C. 2018. "Integration of Information Systems and Cybersecurity Countermeasures: An Exposure to Risk Perspective," *SIGMIS Database* (49:1), pp. 33–52.

Blakley, B., McDermott, E., and Geer, D. 2001. *Information Security Is Information Risk Management*, ACM Press, p. 97.

Caralli, R., Stevens, J., Young, L., and Wilson, W. 2007. "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," No. CMU/SEI-2007-TR-012, Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Choobineh, J., Dhillon, G., Grimaila, M. R., and Rees, J. 2007. "Management of Information Security: Challenges and Research Directions," *Communications of the Association for Information Systems* (20).

Cohen, M. D. 2007. "Reading Dewey: Reflections on the Study of Routine," *Organization Studies* (28:5), pp. 773–786.

Coles-Kemp, L. 2009. "Information Security Management: An Entangled Research Challenge," *Information Security Technical Report* (14:4), pp. 181–185.

Cox, A. M. 2012. "An Exploration of the Practice Approach and Its Place in Information Science," *Journal of Information Science* (38:2), pp. 176–188.

Cram, W. A., D'Arcy, J., and Proudfoot, J. G. 2019. "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance.," *MIS Quarterly* (43:2).

D'Adderio, L. 2011. "Artifacts at the Centre of Routines: Performing the Material Turn in Routines Theory," *Journal of Institutional Economics* (7:2), pp. 197–230.

D'Arcy, J., Herath, T., and Shoss, M. K. 2014. "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *Journal of Management Information Systems* (31:2), pp. 285–318.

Dhillon, G., and Backhouse, J. 2001. "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal* (11:2), pp. 127–153.

Djordjevic, I., Gan, C., Scharf, E., Mondragon, R., Gran, B., Kristiansen, M., Dimitrakos, T., Stølen, K., and Opperud, T. 2002. "Model Based Risk Management of Security Critical Systems," *WIT Transactions on Modelling and Simulation* (31), pp. 253–264.

Douglas, H. 2009. "The Failure of Risk Management: Why It's Broken and How to Fix It," *J. Wiley& Sons, NY* (46).

Feldman, M. S., and Orlikowski, W. J. 2011. "Theorizing Practice and Practicing Theory," *Organization Science* (22:5), pp. 1240–1253.

Feldman, M. S., Pentland, B. T., D'Adderio, L., and Lazaric, N. 2016. "Beyond Routines as Things: Introduction to the Special Issue on Routine Dynamics," *Organization Science* (27:3), pp. 505–513.

Fenz, S., and Ekelhart, A. 2011. "Verification, Validation, and Evaluation in Information Security Risk Management," *IEEE Security & Privacy Magazine* (9:2), pp. 58–65.

Fenz, S., Heurix, J., Neubauer, T., and Pechstein, F. 2014. "Current Challenges in Information Security Risk Management," *Information Management & Computer Security* (22:5), pp. 410–430.

Foroughi, F. 2008. "Information Asset Valuation Method for Information Technology Security Risk Assessment," in *Proceedings of the World Congress on Engineering*, (Vol. 1).

Fredriksen, R., Kristiansen, M., Gran, B. A., Stølen, K., Opperud, T. A., and Dimitrakos, T. 2002. "The CORAS Framework for a Model-Based Risk Management Process," in *International Conference on Computer Safety, Reliability, and Security*, Springer, pp. 94–105.

Gerber, M., and Solms, R. von. 2005. "Management of Risk in the Information Age," *Computers & Security* (24:1), pp. 16–30.

Gerber, M., von Solms, R., and Overbeek, P. 2001. "Formalizing Information Security Requirements," *Information Management & Computer Security* (9:1), pp. 32–37.

Gerber, M., and Von Solms, R. 2001. "Special Features: From Risk Analysis to Security Requirements," *Computers and Security* (20:7), pp. 577–584.

Gherardi, S. 2009. "Knowing and Learning in Practice-based Studies: An Introduction," *The Learning Organization* (16:5), (S. Gherardi, ed.), pp. 352–359.

Gritzalis, D., Iseppi, G., Mylonas, A., and Stavrou, V. 2018. "Exiting the Risk Assessment Maze: A Meta-Survey," *ACM Computing Surveys* (51:1), pp. 1–30.

Haqaf, H., and Koyuncu, M. 2018. "Understanding Key Skills for Information Security Managers," *International Journal of Information Management* (43), pp. 165–172.

Hashim, N. A., Abidin, Z. Z., Zakaria, N. A., Ahmad, R., and Puvanasvaran, A. 2018. "Risk Assessment Method for Insider Threats in Cyber Security: A Review," *Iternational Journal of Advanced Computer Science and Applications* (9:11).

Hedström, K., Kolkowska, E., Karlsson, F., and Allen, J. P. 2011. "Value Conflicts for Information Security Management," *The Journal of Strategic Information Systems* (20:4), pp. 373–384.

Higgins, D. 2009. "Engaging the Small Firm in Learning: Practice Based Theorising on Complex Social Knowledge," *Journal of European Industrial Training* (33:1), pp. 81–96.

Hsu, C. W. 2009. "Frame Misalignment: Interpreting the Implementation of Information Systems Security Certification in an Organization," *European Journal of Information Systems* (18:2), pp. 140–150.

Hyde, K. F. 2000. "Recognising Deductive Processes in Qualitative Research," *Qualitative Market Research: An International Journal* (3:2), pp. 82–90.

ISO/IEC 27000. 2018. *ISO/IEC 27000: Information Technology — Security Techniques — Information Security Management Systems - Overview and Vocabulary*, ISO.

ISO/IEC 27005. 2013. *ISO/IEC 27005: Information Technology-Security Techniques - Information Security Risk Management*, ISO.

ISO/IEC 27005. 2018. *ISO/IEC 27005: Information Technology-Security Techniques - Information Security Risk Management*, ISO.

Kaarst-Brown, M. L., and Thompson, E. D. 2015. *Cracks in the Security Foundation: Employee Judgments about Information Sensitivity*, ACM Press, pp. 145–151.

Kotulic, A. G., and Clark, J. G. 2004. "Why There Aren't More Information Security Research Studies," *Information & Management* (41:5), pp. 597–607.

Kunder, R., and Clarke, N. 2013. "Web-Based Risk Analysis for SMEs," *Advances in Communications, Computing, Networks and Security* (10), pp. 120–127.

Kvale, S. 1996. *InterViews: An Introduction to Qualitive Research Interviewing*, Sage.

Longhurst, R. 2003. "Semi-Structured Interviews and Focus Groups," *Key Methods in Geography* (3:2), pp. 143–156.

Maneerattanasak, U., and Wongpinunwatana, N. 2017. "A Proposed Framework: An Appropriation for Principle and Practice in Information Technology Risk Management," in *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)*, Langkawi, Malaysia: IEEE, July, pp. 1–6.

Marshall, M. N. 1996. "Sampling for Qualitative Research," *Family Practice* (13:6), pp. 522–526.

Mason, J. 2002. "Qualitative Researching," *University of Manchester, UK: Sage Publishings*.

McEvoy, T. R., and Kowalski, S. J. 2019. "Deriving Cyber Security Risks from Human and Organizational Factors – A Socio-Technical Approach," *Complex Systems Informatics and Modeling Quarterly* (18), pp. 47–64.

Mersinas, K., Hartig, B., Martin, K. M., and Seltzer, A. 2016. "Measuring Attitude towards Risk Treatment Actions amongst Information Security Professionals: An Experimental Approach," in *15th Workshop on the Economics of Information Security. University of California Berkeley, Berkeley CA, USA*, pp. 13–14.

Miner, A. S. 1990. "Structural Evolution Through Idiosyncratic Jobs: The Potential for Unplanned Learning," *Organization Science* (1:2), pp. 195–210.

Nicolini, D., Gherardi, S., and Yanow, D. 2004. "Introduction: Toward a Practice-Based View of Knowledge and Learning in Organization," in *Knowing in Organisations: A Practice-Based Approach*, London: M.E. Sharpe, pp. 3–31.

Nieles, M., Dempsey, K., and Pillitteri, V. Y. 2017. "An Introduction to Information Security," No. NIST SP 800-12r1, Gaithersburg, MD: National Institute of Standards and Technology, June.

Niemimaa, E. 2016. "A Practice Lens for Understanding the Organizational and Social Challenges of Information Security Management.," in *PACIS*, p. 58.

NIST SP 800-30. 2012. "Guide for Conducting Risk Assessments," No. NIST SP 800-30r1, Gaithersburg, MD: National Institute of Standards and Technology.

NIST SP 800-39. 2011. "Managing Information Security Risk :: Organization, Mission, and Information System View," No. NIST SP 800-39, Gaithersburg, MD: National Institute of Standards and Technology.

Njenga, K., and Brown, I. 2010. "The Case for Improvisation in Information Security Risk Management," in *E-Government, E-Services and Global Processes* (Vol. 334), M. Janssen, W. Lamersdorf, J. Pries-Heje, and M. Rosemann (eds.), Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 220–230.

Njenga, K., and Brown, I. 2012. "Conceptualising Improvisation in Information Systems Security," *European Journal of Information Systems* (21:6), pp. 592–607.

Nonaka, I., Toyama, R., and Konno, N. 2000. "SECI, Ba and Leadership: A Unified Model of Dynamic Knowledge Creation," *Long Range Planning* (33:1), pp. 5–34. (https://doi.org/10.1016/S0024-6301(99)00115-6).

Oates, B. J. 2005. *Researching Information Systems and Computing*, Sage.

Okoli, C., and Schabram, K. 2010. "A Guide to Conducting a Systematic Literature Review of Information Systems Research," *Sprouts: Working Papers on Information Systems* (10:26).

Orlikowski, W. J. 2002. "Knowing in Practice: Enacting a Collective Capability in Distributed Organizing," *Organization Science* (13:3), pp. 249–273.

Osborn, E., and Simpson, A. 2018. "Risk and the Small-Scale Cyber Security Decision Making Dialogue—a UK Case Study," *The Computer Journal* (61:4), (G. Loukas, ed.), pp. 472–495.

Ozkan, S., and Karabacak, B. 2010. "Collaborative Risk Method for Information Security Management Practices: A Case Context within Turkey," *International Journal of Information Management* (30:6), pp. 567–572.

Pan, L., and Tomlinson, A. 2016. "A Systematic Review of Information Security Risk Assessment," *International Journal of Safety and Security Engineering* (6:2), pp. 270–281.

Parnas, D. L., and Clements, P. C. 1986. "A Rational Design Process: How and Why to Fake It," *IEEE Trans. Softw. Eng.* (12:2), pp. 251–257.

Patton, M. Q. 2014. *Qualitative Research and Evaluation Methods . Thousand Oakes*, ca: sage.

Peltier, T. R. 2005. *Information Security Risk Analysis*, (2nd ed.), Boca Raton: Auerbach Publications.

Peltier, T. R. 2010. *Information Security Risk Analysis*, (3d ed.), Boca Raton, FL: Auerbach Publications.

Pentland, B. T. 2003. "Conceptualizing and Measuring Variety in the Execution of Organizational Work Processes," *Management Science* (49:7), pp. 857–870.

Pentland, B. T., and Feldman, M. S. 2005. "Organizational Routines as a Unit of Analysis," *Industrial and Corporate Change* (14:5), pp. 793–815.

Pentland, B. T., and Feldman, M. S. 2008. "Designing Routines: On the Folly of Designing Artifacts, While Hoping for Patterns of Action," *Information and Organization* (18:4), pp. 235–250.

Ritchie, J., and Spencer. 2002. "Qualitative Data Analysis for Applied Policy Research," in *The Qualitative Researcher's Companion*, A. M. Huberman and M. B. Miles (eds.), Thousand Oaks, CA: Sage Publications, pp. 173–194.

Saleh, M. S., and Alfantookh, A. 2011. "A New Comprehensive Framework for Enterprise Information Security Risk Management," *Applied Computing and Informatics* (9:2), pp. 107–118.

Schatzki, T. R. 2012. "A Primer on Practices: Theory and Research," in *Practice-Based Education*, Rotterdam, The Netherlands: Sense Publishers, pp. 13–26.

Schirrmacher, N.-B., Ondrus, J., and Tan, F. T. C. 2018. *Towards a Response to Ransomware: Examining Digital Capabilities of the WannaCry Attack*.

Schmidt, C. 2004. "The Analysis of Semi-Structured Interviews," *A Companion to Qualitative Research*, pp. 253–258.

Shameli-Sendi, A., Aghababaei-Barzegar, R., and Cheriet, M. 2016. "Taxonomy of Information Security Risk Assessment (ISRA)," *Computers & Security* (57), pp. 14–30.

Shedden, P., Ahmad, A., Smith, W., Tscherning, H., and Scheepers, R. 2016. "Asset Identification in Information Security Risk Assessment: A Business Practice Approach," *Communications of the Association for Information Systems* (39:1), p. 15.

Shedden, P., Smith, W., and Ahmad, A. 2010. *Information Security Risk Assessment: Towards a Business Practice Perspective*.

Silva, F. R. L., and Jacob, P. 2018. "Mission-Centric Risk Assessment to Improve Cyber Situational Awareness," in *Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018*, Hamburg, Germany: ACM Press, pp. 1–8.

Silverman, D. 2015. *Interpreting Qualitative Data*, Sage.

Siponen, M. 2006. "Information Security Standards Focus on the Existence of Process, Not Its Content," *Communications of the ACM* (49:8), p. 97.

Siponen, M., and Willison, R. 2009. "Information Security Management Standards: Problems and Solutions," *Information & Management* (46:5), pp. 267–270.

von Solms, B. 2000. "Information Security — The Third Wave?," *Computers & Security* (19:7), pp. 615–620.

von Solms, B. 2006. "Information Security – The Fourth Wave," *Computers & Security* (25:3), pp. 165–168.

von Solms, B., and von Solms, R. 2004. "The 10 Deadly Sins of Information Security Management," *Computers & Security* (23:5), pp. 371–376.

von Solms, B., and von Solms, R. 2018. "Cybersecurity and Information Security – What Goes Where?," *Information and Computer Security* (26:1), pp. 2–9.

von Solms, R., and van Niekerk, J. 2013. "From Information Security to Cyber Security," *Computers & Security* (38), pp. 97–102.

Spears, J. L. 2005. "A Holistic Risk Analysis Method for Identifying Information Security Risks," in *Security Management, Integrity, and Internal Control in Information Systems* (Vol. 193), P. Dowland, S. Furnell, B. Thuraisingham, and X. S. Wang (eds.), Boston: Kluwer Academic Publishers, pp. 185–202.

Spears, J. L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Q.* (34:3), pp. 503–522.

Straub, D. W., and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, pp. 441–469.

Taylor, R. G. 2015. "Potential Problems with Information Security Risk Assessments," *Information Security Journal: A Global Perspective* (24:4–6), pp. 177–184.

Wangen, G. 2017. "Information Security Risk Assessment: A Method Comparison," *Computer* (50:4), pp. 52–61.

Wangen, G., Hallstensen, C., and Snekkenes, E. 2018. "A Framework for Estimating Information Security Risk Assessment Method Completeness: Core Unified Risk Framework, CURF," *International Journal of Information Security* (17:6), pp. 681–699.

Wangen, G., and Snekkenes, E. 2013. "A Taxonomy of Challenges in Information Security Risk Management," in *Proceeding of Norwegian Information Security Conference/Norsk Informasjonssikkerhetskonferanse-NISK 2013-Stavanger, 18th-20th November 2013*, Akademika Forlag.

Webb, J., Ahmad, A., Maynard, S. B., and Shanks, G. 2014. "A Situation Awareness Model for Information Security Risk Management," *Computers & Security* (44), pp. 1–15.

Webb, J., Maynard, S., Ahmad, A., and Shanks, G. 2013. "Towards an Intelligence-Driven Information Security Risk Management Process for Organisations," in *24th Australasian Conference on Information Systems (ACIS)*, RMIT University, pp. 1–11.

Wei, Y.-C., Wu, W.-C., and Chu, Y.-C. 2018. "Performance Evaluation of the Recommendation Mechanism of Information Security Risk Identification," *Neurocomputing* (279), pp. 48–53.

Whitman, M. E., and Mattord, H. J. 2014. *Management of Information Security*, (Fourth edition.), Stamford, CT, USA: Cengage Learning.

Williams, P. A. 2007. "Medical Insecurity: When One Size Does Not Fit All," *Proceedings of 5th Australian Information Security Management Conference* (Edith Cowan University), December 4th 2007-.

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* (19:1), pp. 21–41.

Paper A

Rethinking capabilities in information security risk management: a systematic literature review

Lundgren, M. (2020) 'Rethinking capabilities in information security risk management: a systematic literature review,' *Int. J. Risk Assessment and Management*, Vol. 23, No. 2, pp.169–190.

Rethinking capabilities in information security risk management: a systematic literature review

Martin Lundgren

Department of Computer Science,
Luleå University of Technology,
971 87 Luleå, Sweden
Email: Martin.Lundgren@ltu.se

Abstract: Information security risk management capabilities have predominantly focused on instrumental onsets, while largely ignoring the underlying intentions and knowledge these management practices entail. This article aims to study what capabilities are embedded in information security risk management. A theoretical framework is proposed, namely rethinking capability as the alignment between intent and knowing. The framework is situated around four general risk management practices. A systematic literature review utilising the framework was conducted, resulting in the identification of eight identified capabilities. These capabilities were grouped into respective practices: integrating various perspectives and values to reach a risk perception aligned with the intended outcome (identify); adapting to varying perspectives of risks and prioritising them in accordance with the intended outcome (prioritise); security controls to enable resources, and integrate/reconfigure beliefs held by various stakeholders (implement); and sustaining the integrated resources and competences held by stakeholders to continue the alignment with the intended outcome (monitor).

Keywords: information security; risk management; capability; intent; knowing.

Reference to this paper should be made as follows: Lundgren, M. (2020) 'Rethinking capabilities in information security risk management: a systematic literature review', *Int. J. Risk Assessment and Management*, Vol. 23, No. 2, pp.169–190.

Biographical notes: Martin Lundgren is a PhD candidate in Information Systems at Luleå University of Technology, Sweden. He received his BSc in Informatics from University of Gothenburg Sweden in 2012, and his MSc in Information Security from Luleå University of Technology in 2014. His general research interests are information security and risk management from socio-organisational perspectives.

1 Introduction

Information security risk management (ISRM) is the routine practice of identifying and assessing security risks and implementing and monitoring controls that address those risks in order to protect organisational interests (ISO/IEC, 2013; Spears and Barki, 2010). Security risks include everything from data loss and leakage to attacks by disgruntled employees, criminal and state-sponsored operations (Ernst & Young, 2012). This article

aims to study what capabilities are embedded in ISRM. Capability is distinguished by 'knowing' and 'intent' (Carlile, 2002; Orlikowski, 2002). Intent refers to the expressed outcome of the risk practice in terms of security controls to preserve an information system's confidentiality, integrity and availability (ISO/IEC, 2013; NIST, 2011). Knowing refers to acting 'knowledgeably' as part of a routine risk practice (Orlikowski, 2002); in other words, what enables people to define, prepare, shape and learn how to solve a task or challenge (Von Krogh et al., 2000). Here, capability is defined and studied by emphasising knowing as the conscious activity for appropriately "adapting, integrating, and reconfiguring internal and external organizational skills, resources, and functional competences" to align with the requirements of an intended outcome [Teece et al., (1997), p.515].

While much attention has been devoted to the challenge of implementing security controls aligned with organisational interests (Halliday et al., 1996; McAdams, 2004), mainly from instrumental approaches (Dhillon and Backhouse, 2001) adopted from best-practices (generic rule frameworks) (ISO/IEC, 2013; NIST, 2011), and how to manage the challenge of organisationally implementing those security measures (Bulgurcu et al., 2010; Siponen, 2000a; Veiga and Eloff, 2010), the literature rarely discusses the actual routine practices (Shamala et al., 2015; Shedden et al., 2010; Siponen, 2006; Taylor and Brice, 2012). Despite (or because) prior research has long emphasised routine security risk practices to manage various security challenges (Baskerville, 1991; Chen et al., 2011; Hirsch and Ezingeard, 2008; Rainer et al., 1991; Spears and Barki, 2010), the capabilities comprising those practices remain riddled with ambiguities. For example, some scholars recognise employees as great assets in the effort to reduce security risks because of their unique business knowledge (Albrechtsen and Hovden, 2010; Johnson and Johansson, 2008). Others frame employees as serious security risks (Posey et al., 2011; Warkentin and Willison, 2009). Some scholars promote technical controls and expert knowledge (Birch and McEvoy, 1992; Vermeulen and Von Solms, 2002), while others favour social factors and advocate for socio-organisational approaches (Crossler et al., 2013; Dhillon and Backhouse, 2001). Because capabilities in security risk practices ultimately determine what security measures to adopt and how, addressing this discussion remains critical for information security practitioners and researchers alike. For this reason, it is necessary first to examine the existing ISRM literature to understand what capabilities are embedded in its routine practice.

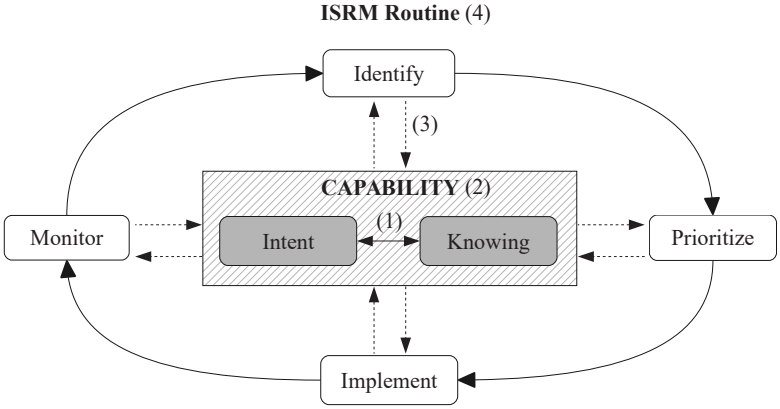
Contributing to this discussion, ISRM routines are analysed from a practice perspective. Drawing on a practice-based approach (Carlile, 2002), this article studies how risk practice capabilities are constructed by the intended outcome and underlying knowledge. The remainder of the article is organised into four sections. Following the introduction, Section 2 presents a theoretical framework for analysing the literature. Section 3 presents the method for the systematic review and surveys routines and capabilities in risk management research. Section 4 presents the findings, and Section 5 discuss their implications. Section 6 highlights the contributions of this paper.

2 Theoretical framework

Routine ISRM capabilities have predominantly consisted of 'what works' types of questions: what interventions, controls and strategies should be used to meet specific policy or compliance intentions (Dhillon and Backhouse, 2000, 2001; Njenga and Brown,

2012; Siponen, 2002). The literature on ISRM capabilities has largely ignored, however, the underlying knowledge behind intentions and what ultimately enables people to achieve that knowledge (Shedden et al., 2011; Siponen, 2000b; Spears, 2006). A practice-based perspective (risk-as-practice) tries to link these two dimensions as the intent of the risk practice and the knowledge on which the practice is based. Risk-as-practice regards routine ISRM capabilities as ongoing activities and accomplishments as something people do, rather than something organisations have – 'what works' – in terms of established security measures and controls (Whittington, 2006). To study what capabilities are embedded in ISRM routines, a simple framework was developed (see Figure 1). The framework was inspired by Carlile (2002) and Orlikowski's (2002) discussions on knowledge structures in practice, as well as four general routine risk practices: identifying, prioritising, implementing and monitoring (ISO/IEC, 2013; Shedden et al., 2010; Spears and Barki, 2010). In the framework, the capability of routine ISRM practices is constructed by its relation to 'knowing' – the ability to define, prepare, shape and learn to solve a task or challenge – and 'intent' – the intended future conditions that shape the practice in the present (Kornberger and Clegg, 2011).

Figure 1 Theoretical framework to describe the relation between routine risk practices and capability



The intent of information security risk practices can be described as the desire for, and the awareness of, fulfilling a future outcome (Malle and Knobe, 1997). It is shaped by the practitioner's belief, perception and attitude towards risks (Bulgurcu et al., 2010; Hirsch and Ezingeard, 2008). Knowledge is the precondition of intent, as it is exercised in situations to ascribe sense to the practice (Feldman et al., 2016). However, knowing is also influenced by intentions. For example, knowledge can be intentionally sought during a crisis and as such be shaped by that intention (Malle and Knobe, 1997; Orlikowski, 2002). The alignment between the *intent to do* and *knowing how to do* is what constitutes capability. This alignment is marked with the bold bidirectional arrow (1) in the theoretical framework.

Capability (2) is thus generated through engagement in practice; it is the conscious activity of adapting, integrating and reconfiguring skills, resources and competences to reach an intended future condition. Just as intent and knowing should not be seen as static, nor should capability; rather, it is an ongoing accomplishment that is constructed and reconstructed as practitioners engage in the practice (Orlikowski, 2002). A capability's continuity is achieved as people engage in reoccurring practices, thus 'encoding' the knowledge into routine (Levitt and March, 1988; March, 1991). Hence, capability is not something that an organisation has, but something that can be generated by people through practice as a product of intentions and knowledge. Misalignment between capability and routines has been shown to affect practice compliance and to be related to intent and knowledge (Bulgurcu et al., 2010). Likewise, alignment between capability and routines can be achieved over time by adapting and reconfiguring intent and knowledge with stable, routine practices (Berente et al., 2016). The relationship between capability and routine practices is marked with two unidirectional arrows (3), where capability shapes and is shaped by the enactment of routine practice (Feldman and Pentland, 2003).

The following section describes the repetitive, recognisable patterns of practices that comprise the ISRM routine (4). Identification, the first routine risk practice, seeks to identify critical organisational assets and associate plausible risks in order to adequately determine how, where and why something could happen (ISO/IEC, 2013; Spagnoletti and Resca, 2008). Assets include any element of relevance to an organisation's system, including people, procedures, data, information, software, networks, etc. (Whitman and Mattord, 2014). Risks include threats and vulnerabilities that could potentially compromise an information system's confidentiality, integrity or availability, whether logical or physical, internal or external, human or non-human or accidental or intentional (Bandyopadhyay et al., 1999; Shedden et al., 2010). This enumeration of risks has been criticised, however, for neglecting social factors (Dhillon and Backhouse, 2001), such as knowledge sharing and communication (Padyab et al., 2014; Webb et al., 2016), making it difficult to ensure that an organisation's risk managing intentions are aligned with actual practices (Hirsch and Ezingeard, 2008). A high risk identification capability depends on more than adequately determining what assets are most critical, what threats and vulnerabilities the organisation faces or what existing security controls are in place. Moreover, it must know, what sets of competencies, knowledge and resources exist to reach the intended outcome (Shedden et al., 2011).

The second routine risk practice, prioritising, seeks to analyse the relationship between each identified asset and its associated risks in order to prioritise and determine if and what mitigation action to deploy (ISO/IEC, 2013; Spagnoletti and Resca, 2008). This criticality is prioritised based on consequences, impact and likelihood of successful risk exploitation. Estimating consequence and impact requires determining the most prescient risks for the organisation, recovery costs, prevention expenditures, etc. (Shedden et al., 2010; Whitman and Mattord, 2014). This challenge is typically addressed by measuring risks either quantitatively by comparing the costs of mitigation with the likelihood of exploitation or qualitatively in terms of the perceived impact of the information system's loss, corruption or unavailability (Visintine, 2003). The intention to adequately prioritise risks is a matter of knowing the trade-offs between risk acceptance and tolerance (NIST, 2011). When considering, for example, regulations around privacy

and data protection, some risks might be acceptable from an organisation's operational perspective, but intolerable from a legal perspective. The likelihood and consequences of a particular risk are considered in regards not only to the flow and operational efficiency of the information systems but also to laws, legislations, ethics, costs, policies, standards, compliances, etc. The effectiveness of prioritising risks, however, can be problematic. As many organisations consider information about breaches, security compromises, losses and frequency to be sensitive and confidential, reliable empirical data are in short supply (Baskerville, 2005). Hence, knowing how to integrate various perspectives on both resources and competencies is necessary to adequately achieve the intended outcome.

The third routine risk practice, implementing risk-reducing controls, seeks to provide a consistent, organisation-wide response to risks in relation to their priority (NIST, 2011; Shameli-Sendi et al., 2016). Controls for information security include any "process, policy, procedure, guideline, practice or organisational structure, which can be administrative, technical, management, or legal in nature which modify information security risk" [ISO/IEC, (2013), p.2]. The resulting risk response can take various forms; it can, for example, include mitigating (to change the likelihood or consequence of risks by manipulating, limiting or removing vulnerabilities, access or security controls), transferring (to shift the risk to other assets, processes or organisations, like outsourcing or insurance), accepting (risks outcome of a successful exploitation may or may not be consciously retained) or terminating (to remove the source of risk entirely to avoid exploitation) (ISO/IEC, 2013; Whitman and Mattord, 2014). The capability to implement relevant controls with an adequate risk response requires the competency to consciously challenge the risk source and is grounded in the skill and knowledge needed to reconfigure present conditions to align with the intended future outcome (Njenga and Brown, 2012).

The last of the four routine risk practices, monitoring, seeks to survey risks and their factors (assets criticality, impact, likelihood, legal and environmental contexts and implemented controls) to review and identify changes (ISO/IEC, 2013; Shameli-Sendi et al., 2016). Because risks are never static, their factors can change at any time. Routine monitoring therefore aims to maintain awareness of an organisation's risk environment and associated activities to support risk decisions (ISO/IEC, 2013; NIST, 2011). Risk monitoring surveys the ongoing effectiveness of the risk practices and helps verify the sufficiency and compliance of implemented controls (NIST, 2011). This is not to say, however, that compliance equals information security, which is a growing misconception (Webb et al., 2016). Monitoring capabilities integrate and adapt resources and competencies to increase risk awareness and alertness (Werlinger et al., 2010). Monitoring also oversees present conditions and their alignment with the intended outcome of risk practices.

3 Research method

The research method was based on a concept-centric approach using Ritchie and Spencer's (2002) framework of analysis and Okoli and Schabram's (2010) steps for conducting a systematic literature review as a predefined search protocol (Kitchenham, 2004).

Search strategy

Since this article seeks to survey what capabilities are embedded in routine risk practices, the search strategy targeted articles with descriptive qualitative attributes. This approach affected the gathering of articles, as qualitative literature is text-based, rich in meanings and reflective of only partial studies and the findings (Tranfield et al., 2003). Consequently, the search was not limited to a particular study design, time frame or journal (Dixon-Woods et al., 2006; Webster and Watson, 2002). However, because risk management is influenced by human behaviour that constitutes the work practices, the review saw fit to undertake a more socio-organisational view and delimit the data collection outlets only to established top journals within the information systems field[1] using the following search phrases: 'information security' AND ('risk management' OR 'risk practice' OR 'risk mitigation' OR 'risk assessment')[2].

Practical screening

The resulting articles were first examined by their titles and abstracts. Only articles reflecting or discussing ISRM practices were kept and subjected to detailed examination by the following criteria. For inclusion, a) the article must be written in English and b) must be within the scope of information security. For exclusion, a) articles reflecting on information security issues or challenges outside the scope of risk management practices (workshop or benchmark studies, for example) and b) study proposals, commentaries and literature reviews not related to risk management practices were excluded.

Quality appraisal

This article aimed to study what capabilities are embedded in ISRM routine practices. Since underlying intent and knowledge on an individual level are out of the scope of a literature review, intent was, if not otherwise expressed, associated with achieving recommendations found in common security management standards, in particular ISO/IEC (2013) and NIST (2011), as described in Section 2. Capability was thus studied as the ability to adapt, integrate and reconfigure skills, resources and competences to achieve these intended future conditions (Teece et al., 1997). Because the research question focused on understanding *what* rather than *if* or *how* questions, no relevant article should be excluded due to its quality unless fundamentally flawed. The appraisal thus looked at the claims and supporting evidence (Hart 1999, as in Okoli and Schabram, 2010).

Data extraction and synthesis

The data extraction method saw fit to follow the systematic process of Ritchie and Spencer (2002), as the approach segments summarising data into predefined categories in an existing theoretical framework. Ritchie and Spencer's framework consists of five phases and was applied as follows. *Familiarisation*: the articles were read and key concepts were noted together with ideas and motivations for emerging themes. *Identifying a thematic framework*: this stage can be used to create new theoretical frameworks but may be excluded if an existing framework is used, as in this case. *Indexing*: data were extracted by associating capabilities within any of the four routine

risk practices as outlined in the theoretical framework discussed in Section 2. *Charting*: the extracted data were summarised into a spreadsheet, 'lifting' the data from the original context and into a concept-matrix, mapping the routine risk practice, intent and knowledge. *Mapping and interpretation*: in the final phase, differences, relations and parallels in the data and between categories were explored and synthesised. Finally, the extracted data were read and reread within the concept-matrix and together with notes from the familiarisation phase identified protruding themes. The identified themes were then grouped and synthesised into respective practices.

4 Capabilities in risk practice

This section presents the result of the practical screening and Ritchie and Spencer's framework. The search strategy resulted in a total of 73 articles (18 from EIJS, 14 from ISJ, 3 from JAIS, 5 from JIT, 22 from JMIS, 3 from JSIS and 8 from MISQ). The practical screening rejected 46 of these articles (3 not available online, 3 cover-pages, and 40 outside the scope of ISRM practices), resulting in a total of 27 articles analysed.

Table 1 An overview of the number of articles found and included from the targeted journals

Journal	*Hits*	*Available*	*Included*
EIJS – European Journal of Information Systems	20	18	5
ISJ – Information Systems Journal	14	14	4
JAIS – Journal of the Association for Information Systems	3	3	2
JIT – Journal of Information Technology	5	5	2
JMIS – Journal of Management Information Systems	23	22	8
JSIS – Journal of Strategic Information Systems	3	3	0
MISQ – MIS Quarterly	11	8	6
Total	79	73	27

From the analysed literature, various capabilities (the knowledge needed to achieve intended outcomes) within each routine practice were extracted. Eight capabilities were identified that reflected the themes of adapting, integrating and reconfiguring skills, resources or competences that affect the outcome of a given practice.

Table 2 Eight capabilities as identified from the analysed literature

Identify	*Prioritise*	*Implement*	*Monitor*
• Integrating different perceptions • Integrating different information values • Adapting to different desired outcomes	• Knowing the risk trade-offs	• Understanding adequate controls • Integrating beliefs and held values	• Preserving compliance • Risk reduction alertness

Table 3 summarises in one sentence each practice capability based on the data extraction and theme.

Table 3 A summary of the identified capabilities from each ISRM practice

Identify	*Prioritise*	*Implement*	*Monitor*
The capability to integrate various perspectives and values to reach a risk perception aligned with the intended outcome.	The capability to adapt to varying perspectives of risks and prioritising them in accordance with the intended outcome.	The capability to adapt security controls to enable resources, and integrate/reconfigure beliefs held by various stakeholders.	The capability to sustain the integrated resources and competences held by stakeholders to continue the alignment with the intended outcome.

The following section summarises the analysis based on the four general ISRM routine practices (identify, prioritise, implement and monitor) as discussed in Section 2. The analysis is segmented by the identified themes to better highlight the different capabilities.

4.1 Identify

4.1.1 Integrating different perceptions

Moving beyond the traditional view of ISRM as relying solely on technical solutions, authors prioritising socio-organisational elements when identifying risks in their research have devoted much attention to employees. The literature generally has two perspectives on employees, seeing them as either a serious security risk (Lowry and Moody, 2015) or a great asset in the effort to prevent risks (Spears and Barki, 2010). Although the two perspectives express opposite views, the intention to identify and control risks is similar. For example, Lowry and Moody (2015) argue that mitigating some identified risks can lead to freedom restrictions, which can cause users to act undesirably, creating new risks. Similarly, Spears and Barki (2010) argue that employees often have necessary business knowledge that can lead to more effective security controls and that their participation leads to more engaged employees. In other words, varying perceptions or values (Dhillon and Torkzadeh, 2006) have been expressed to facilitate alignment between intent and security risk practices.

In their article on value-focused information security, Dhillon and Torkzadeh (2006) focused on 'what we care about' questions rather than addressing security solely from normative objectives. Dhillon and Torkzadeh (2006) argue that value informs the relative desirability of consequences and can help managers create value-based security controls rather than being limited to standard alternatives. An example of the benefit of adopting different perceptions and competences in the risk identification routine is provided in one of Spears and Barki's interviews with a chief information security officer. As he explained, "I don't understand the business like they [the employees] do, so I don't understand the information. I don't understand the relative importance of the information. I don't understand the context of the information in the way people do their daily business, so I don't know what forms people need the information in, how readily accessible it needs to be, how it flows through the business processes, and therefore where the critical junctures are that need to be controlled" [Spears and Barki, (2010),

p.510]. Integrating different perceptions, such as "what we care about" (Dhillon and Torkzadeh, 2006), can emancipate those oppressed by security controls (Lowry and Moody, 2015) and help to address them as assets rather than risks (Spears and Barki, 2010).

4.1.2 Integrating different information values

Traditionally, risk management aims first to identify risks towards a business by cataloguing all threats to information assets and communication between information systems. These threats are commonly classified according to confidentiality, integrity and availability-frequently referred to as the CIA triad (Birch and McEvoy, 1992). Straub and Welke's (1998) study on risk management found that the traditional CIA triad was not equally prioritised in practice, as confidentiality was by far the most frequently discussed among the organisations targeted by the study. Top managers stressed the need to find controls that could improve authorisation and access control to information. Interestingly, in contrast to the findings of Straub and Welke (1998), Dhillon and Torkzadeh's (2006) study composed of interviews with managers from a broad cross-section of industries, found that data integrity alone was a reoccurring theme from the traditional information security practice. These managers understood availability as a means objective and confidentiality as the established ownership of information, which reflects different perceptions of what should be protected. Using the CIA triad as the cornerstone of risk management can cause managers to overlook or ignore other organisationally grounded security vulnerabilities and problems. Similarly, Goldstein et al. (2011) argue that the traditional information security perspective is over emphasised. They suggest that an organisation's reputation, after a successfully exploited risk, is more negatively impacted if the organisation's functionality (availability or integrity of information) is affected, rather than the confidentiality of information.

This perspective assigns risk effects solely to the business operation, where the desired outcome of the information security risk practice is to enable an organisation's operational efficiency. However, the desired outcome of ISRM routine risk practices could also rest with other stakeholders, like the users of a service (Culnan and Williams, 2009; Oetzel and Spiekermann, 2014). From such a perspective, the effect of a certain risk could be seen as transferred, framing the users of a service as those ultimately at risk, while positioning the organisation as the threat landscape. An online service, for example, may need to share certain user information with third parties, thus potentially exposing users' information to risk. Users may have no knowledge of the risks they incur when providing their information to the service. This creates a managerial difficulty in balancing the users' privacy and the right and legitimate needs of others. As a result, Culnan and William addressed privacy as a major part of information security management, stressing the importance of confidentiality to counter the harm of information abuse and unauthorised access. The authors also concluded that organisations dealing with improving privacy behaviours should create a top-down culture of privacy from an accountable governance process and avoid decoupling privacy from personal experience.

Oetzel and Spiekermann (2014) present a different view on common risk identification practices by including privacy. The privacy perspective of risk management concerns legal compliance and includes auditors, lawyers and data protection officials. However, privacy risks are largely ignored by most risk practices, resulting in a mismatch

between identified privacy risks and implemented controls. Consequently, Oetzel and Spiekermann (2014) incorporated a risk perspective into the ISO risk management standard. The intended outcome of privacy risks, referred to as privacy targets (e.g., systems characterisations), primarily came from existing laws and regulations, such as the EU Data Protection Directives, but also challenged stakeholders to reconfigure privacy infringement because of privacy subjectivity. Because of this subjectivity, organisations should prioritise each privacy target by integrating both an organisational damage perspective (reputation and brand or financial situation) and a privacy-subject perspective (an affected person's social standing and reputation, financial situation or personal freedom) on a scale comprising limited, considerable or devastating effects. The value of information could thus be seen as subjective, and integrating various values could reveal what risks are relevant for a particular stakeholder and organisation.

4.1.3 Adapting to different desired outcomes

Just as information can have different values for different stakeholders, so can the expected outcomes of risk practices. As Rainer et al. (1991) suggested, the highly subjective nature of risk identification could potentially cast doubt on its accuracy and make managers unwilling to base important decisions on them. This could arguably be the result of varying expectations of the risk practice outcome. Hsu (2009) conducted a case study on the perceptions and assumptions of different stakeholders regarding information security standards and certification. Hsu showed that misalignment between intentions and information security controls might cause them not to be fully embedded in the day-to-day work of organisations. In the case study, three groups – the team responsible for the certification process, stakeholders and other employees – were all found to have varying perceptions of the intended outcome. Interestingly, varying perceptions of the intended outcome can be found in many studies and seem to affect actual practices.

For example, the certification team in Hsu's study sought external competencies to better understand the potential risks for the organisation. Although existing security controls were in place, the certification team was not sure that they were compliant. As a result of interacting with external consultants, the certification team increased their knowledge about risk management and security measures. However, because of time limitations, the certification team did not feel they had adequate resources or time to integrate already existing knowledge from people working in other departments. In a similar case by Hsu et al. (2014), the organisation created a new position to facilitate knowledge about risks. Each department manager made appointments on the basis of their domain's knowledge and leadership abilities and took turns filling the position. This initiative helped share knowledge by addressing the gap between the intended outcomes of information security standards, and the knowledge needed to achieve it.

Likewise, Spears and Barki's (2010) study on employees' participation in risk management found that although internal auditors, risk managers and external consultants led the risk management work, employees provided valuable insight into in-depth business activities. This insight helped create new security controls where none had previously existed and reconfigured existing controls based on a 'reality check' provided by the employees. The gap between the actual business process and the intended outcome of the information security risk practice was addressed by integrating employees' competencies. In their case study on improvisation in information security practices,

Njenga and Brown (2012) also integrated various competences. They created a model to categorise data by listing items of criticality and potential risks for which managers then developed creative scenarios. The flexibility of using scenarios "created cognitive knowledge that would potentially be ideal for feedback, leaving practitioners open to determine innovative solutions" [Njenga and Brown, (2012), p.603]. As new risks arose or the environment changed, managers jointly developed new scenarios and built new creative solutions. Similarly, in their study on critical risk factors to assess impacts of e-commerce on overall enterprise risk, Sutton et al. (2008) created focus groups to identify threats by creatively coming up with risk factors that were then tested for consistency between the focus groups. These studies suggest that adapting and integrating the intent and knowledge of various stakeholders can affect the outcome of the security risk practice.

4.2 Prioritise

4.2.1 Knowing the risk trade-offs

The next step in the information security risk practice routine is to assign a level of impact to all of the identified threats. Traditionally, these threats are measured by different means, including cataloguing vulnerabilities and their estimated probability (Birch and McEvoy, 1992). The impact level of threats can be expressed either qualitatively or quantitatively by various formulas. The advantage of a quantitative measurement is that it allows the risk practitioner to identify precisely the assets most critical to the operation of the organisation. Alternatively, when exact figures cannot express risks and their costs, a qualitative method, such as scenarios, can better reflect risks (Rainer et al., 1991).

However, it is not always possible to measure risks, as some are simply unknown or surrounded by too much uncertainty (Cavusoglu et al., 2008; Sun et al., 2006). Instead, the priority is to identify what risks to tackle first, based on their probability and the value of the underlying asset being threatened (Oetzel and Spiekermann, 2014). This step, however, is often based solely on the experience of information security risk practitioners to know what is important, especially during new or uncertain situations (Njenga and Brown, 2012).

Risks and mitigation efforts are commonly prioritised based on the weakest link in order to determine the extent of the organisation's overall security. Kumar et al. (2008) offer an alternative view, namely that an organisation's overall security can be seen as the interaction between security controls, the business environment and risk (Galbreth and Shor, 2010; Sun et al., 2006; Wolff, 2016). According to Kumar et al. (2008), it comes down to the business and threat environments. For example, if a company has an e-commerce website, the value of that website is higher when the number of users is high. The objective of risk management is to ensure business continuity, even if under attack. The priority is to consider interactions between the organisation's business environment and the threat environment. For example, information integrity and availability can have a lower economic impact from security risks than breaches of confidentiality (Goldstein et al., 2011) because the latter does not significantly affect the firm's market value. This contradicts previous beliefs that security risks related to confidentiality are more important (Straub and Welke, 1998).

The risk definitions discussed above estimate or prepare for negative outcomes, but they neglect another important aspect, the level of uncertainty regarding whether the outcome of a risk will be positive or negative (Sun et al., 2006). Galbreth and Shor (2010) argue that the trade-off between risk acceptance and tolerance can also be purely strategic, as shown in their study on software vendors and their products' vulnerabilities. Galbreth and Shor (2010) propose that some vulnerabilities can be positive from a competition perspective. Should an organisation choose to address all security issues, too much time and money will go towards mitigating vulnerabilities; depending on the organisation's market share, this might not be the best option. However, companies with a monopoly have an advantage in addressing all security issues, as they can extract the value of this enhanced security through higher prices. Knowing the risk trade-off comes down to firm values: what risks are important, or "what we care about" (Dhillon and Torkzadeh, 2006).

4.3 Implement

4.3.1 Understanding adequate controls

Once all identified risks are prioritised, risk-reducing controls can be selected and implemented to either eliminate or mitigate exploitation. However, one of the biggest challenges in information security is a firm's lack of knowledge about the full range of available and effective security controls to meet a specific risk priority, ultimately causing managers to adopt inadequate protection (Straub and Welke, 1998). Other studies have highlighted the challenge of adequately meeting the intended risk priority (Oetzel and Spiekermann, 2014). In their case, Oetzel and Spiekermann (2014) presented a scale ranging from satisfactory to very strong to evaluate the security controls established to maintain privacy. The mitigation scale is directly related to a risk's perceived consequences. For example, limited consequences need only satisfactory controls, while devastating consequences need very strong controls. The difference between these types of controls or how to interpret them is not elaborated further. This type of misalignment between intent and knowledge has been shown to affect practice.

For example, Njenga and Brown (2012) found that even though many of the security standards used today, such as ISO and NIST, specify concrete actions, practitioners at times must act spontaneously and improvise. If, for example, information access rights needed to be changed quickly on a request from a department with one type of authority, such as Human Resources (in assigning job descriptions), it could conflict with other departments, such as IT (in assigning group profiles) or the Information Security Officer (in assigning policy), leaving the practitioner with the task of trying to adapt and reconfigure existing security controls (Njenga and Brown, 2012).

Risks can also be countered by means other than trying to reduce or avoid them, such as by reconfiguring the risk source (Birch and McEvoy, 1992). Zhao et al. (2013) discuss transferring risks as a security control. The authors compare three commonly used transfer controls: third-party insurance, risk pooling arrangements (a mutual form of insurance where the policy holder remains the owner) or a managed security service (outsourcing the security risk management). Both third-party insurance and managed security services completely transfer the risk to a new owner. In risk pooling,

organisations within that pool share risks and can thus integrate the competencies of each member organisation to tailor unique security policy terms. The authors do not elaborate on what constitutes adequate controls, instead highlighting the competences for reconfiguring existing or integrating new resources to meet a specific risk's priority level.

4.3.2 Integrating beliefs and held values

As for actual implementation, some scholars argue that the real difficulty is convincing top managers to invest in security measures, given the conception that they will have no return on investment and will be unpopular with employees who must adapt to new rules and processes in their day-to-day work (Rainer et al., 1991). Bulgurcu et al. (2010), Dhillon and Torkzadeh (2006), Hsu et al. (2014) and Spears and Barki (2010) have shown, however, that this is not always the case.

Integrating the competencies of other stakeholders has been shown to provide valuable insights into the implemented controls to see if they 'make sense' in the day-to-day business environment (Spears and Barki, 2010). For example, Bulgurcu et al. (2010) recognised that seeing employees as assets, rather than a security risk, for improving information security helped emphasise the factors motivating employees to comply with information security procedures. Bulgurcu et al. (2010) found that the level of education and technology knowledge, organisation size or type and information intensity of the organisation had no significant impact on users' compliance. Rather, they showed the effect of reconfiguring employees' beliefs about intended outcomes on costs and benefits, safety and vulnerability. In their risk practice study for a major bank, Hsu et al. (2014) similarly described how implemented risk management procedures and regulations gained support by building on the bank's low risk tolerance culture and thus won the support to reconfigure and adapt to these changes.

The different beliefs and perceptions that underpin the intentions for a particular security outcome can be diverse, even within the same organisation. In their case study on an organisation in the public sector, Tsohou et al. (2015) found that managers had varying views of the outcome of risk practices. Some saw the implemented security awareness controls as a method of self-defence; others expressed no concern about external threats but showed more reservation towards internal users or saw security controls as a set of rules and procedures in case of security incidents or disasters to limit reputation damage. This misalignment leads to uneven knowledge and the implementation of security controls; consequently, a firm's security is strengthened only by the initiative of individuals. Integrating beliefs and held values are thus important, as varying perspectives on outcomes can harm security (Dhillon and Torkzadeh, 2006; Tsohou et al., 2015). Dhillon and Torkzadeh found that security controls need to make operations easier for the end user; otherwise, creativity on the part of the employees could lead towards circumventing those same security controls, creating an even greater security risk. Hsu et al. (2014) noted that one attempt to mitigate this risk was to promote awareness by passing out a handbook for employees, showing examples and stories to help them identify risks and follow steps to mitigate them, creating a risk management 'self-assessment' culture.

4.4 Monitor

4.4.1 Preserving compliance

After the identified risks have been prioritised and various controls have been implemented (including process, policy, procedure, guideline, practice, etc.), the monitoring phase aims to give feedback on the success of and compliance with the implemented controls. Some scholars have identified the users of an information system as its weakest link and thus a serious security risk. To address this risk, many organisations follow strict information security policies and implement technical controls designed to decrease information abuse. However, it has been suggested that these security controls are only partially effective because of ignorance. Lowry and Moody (2015) propose a control-reactant compliance model, showing that security controls can be a positive factor motivating the intent to comply but that threats towards personal freedom can result in increased information abuse. Chen et al. (2012) agree that organisations' information security efforts are threatened by employees' negligence and insider breaches and that technological solutions are not enough to solve the situation alone. Management has traditionally targeted insider threats by various security controls, including policies and technical controls. However, employees in general do not seem motivated to follow the established security controls if they get in the way of their day-to-day work. Controls built on both punishment and rewards have been studied, although with inconsistent results. Chen et al. showed that punishment did not motivate compliance with the policy, concluding that employees' outcome beliefs in terms of a reward play a significant role in their compliance.

Other scholars see users of an information system more as rational decision makers that need motivation. For example, Li et al. (2014) proposed a comprehensive framework comparing two distinct approaches to achieving compliance, either a sanction-based (rule adherence, 'command-and-control' to determine user behaviours based on the cost of misbehaviour) or a self-regulatory (users values, ethics and feelings of responsibility towards the organisation) approach. The researchers conducted an online survey to study employees' internet usage and intent to comply with policy. The study showed that self-regulatory forces, including ethics and justice beliefs, motivated employees' policy compliance. Sanctions were shown to be less effective. Similarly, Herath and Rao (2009) found that employees' perception about the severity of breaches and response efficacy, self-efficacy and response costs are likely to affect policy attitudes. These attitudes are also influenced by organisational commitment. Moreover, employees tend to underestimate the probability of a security breach. Hsu (2009) found that users and managers sometimes thought that security measures were only an effort to minimise technical and operational errors, rather than improve employee knowledge and behaviour. This resulted in compliance being more inconvenient than beneficial, motivating some employees to work around the security controls. Tsohou et al. (2015) also concluded that the lack of security intentions stemmed from existing organisational structures and norms that were not aligned with intended security practices. Lowry et al. (2015) examined why users sometimes blame the organisation for their inability to remain compliant with security regulations, concluding that organisational trust was a major driver for decreasing computer abuse.

4.4.2 Risk reduction alertness

In Straub and Welke's (1998) study on coping with systems risks, interviewees did not engage in proactive activities as part of risk management, nor did they take into account feedback to reconfigure or adapt to new control activities. The security action cycle introduced by Straub and Welke (1998) aimed to integrate knowledge about how to deal with risk responses so that controls would consider the public prosecution of an abuser, which would also act as feedback. Spears and Barki (2010) argued that, by including users in the identification and implementation phase, users subsequently felt more personally responsible, promoting more alignment and compliance with the security controls. Hsu et al. (2014) concluded that users were motivated to conduct risk management self-assessments. The risks and controls used to mitigate them were then documented, making it possible for employees to update their assessments in real time. This approach shifted the focus from just having employees comply with the risk procedures to actively engaging them in looking out for new risks and possible ways of mitigating the risk. Njenga and Brown (2012) argued that capturing, monitoring and reporting security incidents depend on various competences in the organisation and that something that should be reported by anyone who noticed anything did not align with the intended security outcome.

Although many companies have legal or policy responsibilities to protect certain information, such as personal information, such regulations are often phrased so that organisations are judged to be compliant if they implement and maintain reasonable procedures. It is difficult, however, to determine what constitutes reasonable or appropriate (Culnan and Williams, 2009). This leaves organisations more concerned with being compliant than actually mitigating threats, which is more appealing in immature operational organisations, whereas mature operational organisations maintain their own security practices based on unique potential risks rather than just following compliance regulations (Kwon and Johnson, 2013). Interestingly, research and security standards have provided insight and guidance for how management and users should operate and use information systems to stay compliant (Smith et al., 2010). However, these compliance frameworks sometimes show gaps in certain circumstances; in the case of Njenga and Brown (2012), they left information security practitioners with the task of adapting to situations and using their own experience to determine what is important and how to stay compliant. Considering that good compliance does not necessarily mean good security, but that good security based on risk management leads to good compliance (Kwon and Johnson, 2013), this gap is important.

5 Discussion

This article contributes to the existing ISRM literature by proposing a theoretical framework to study what capabilities are embedded in routine risk practices. Analysing the literature, the framework produced eight capabilities as the result of what people do in terms of intent and knowledge, rather than something that organisations have. The analysis suggests that ISRM capabilities are a socially constructed alignment between adapting and integrating intent and the knowledge to achieve the intended outcome. That is not to say that any combination of intention and knowledge leads to a capability, but rather that every capability is the result of intention and knowledge. The relation between

intent and knowing is bidirectional, meaning that intentions and knowledge shape and are shaped by each other. The theoretical framework also suggests that capability is the enactment of a certain practice and that intent and knowledge shape and are shaped by the outcome of that practice.

The relation between intent and knowledge can be seen in the *capability to integrate various perspectives and values to reach a risk perception aligned with the intended outcome*. For example, Dhillon and Torkzadeh (2006) suggested that intent can be a starting point for creating security controls rather than being limited by standard alternatives. However, to make this change, managers would have to seek that knowledge from outside or within the organisation in order to adapt to it. This particular capability was noted as *integrating different perceptions*. Because knowledge is not created in vacuum but is exercised in situations that give sense to the practice (Feldman et al., 2016), adapting new knowledge to achieve a certain intent is also affected by the *different desired outcomes* that may exist. To this end, in the work of Hsu et al. (2014) and Hsu (2009), the accrual of additional knowledge aligned security controls with the intent of different stakeholders; in the research of Spears and Barki (2010), employees' knowledge directly helped to shape the risk practice as a 'reality check'. These examples align with the theoretical framework in suggesting that intent and knowledge can constitute a capability when enacted in practice. However, the practical implication has been largely downplayed, this may relate to research being focused on theory. Whilst prior research affirms nuances of *intent to do* and *knowing how to do*, the shortcoming is seeing the potential for a fuller explanation of capabilities. By not having the identified capabilities, each one of them could potentially act as a challenge instead. For example, not *integrating different information values*, as illustrated by Spears and Barki (2010), undermines employees' knowledge about day to day operations. This, in turn, makes establishing *adequate controls* and motivating intent to *preserve compliance* more challenging because of gaps between day to day operations and security measures (Dhillon and Torkzadeh, 2006; Ohki et al. (2009). Of course, capability can only be associated with intent and knowing on a conceptual level, not in an instrumental sense as otherwise argued in much of the earlier ISRM literature. For example, the capability to *integrate different information values* questions the intention and shaping of the risk practice from a subjective point of view, asking, what do we care about? In other words, capabilities do not define a particular set of steps or actions to take and follow, but rather what enables or constrains a certain practice. How capabilities are embedded in routine risk practices remains an open question, however, and further research should investigate how intent and knowing can be developed into capabilities in practice.

Beyond alignment between intent and knowing, perhaps more interesting is the misalignment found in the *capability to adapt to varying perspectives of risks and prioritise them in accordance with the intended outcome*. The literature seems to reflect a general misalignment between intent and knowing in the prioritisation of risks. For example, prioritising risks has traditionally been described as a trade-off between acceptance and tolerance, often expressed instrumentally by comparing the criticality of assets with the probability of risk to best maintain organisational efficiency (NIST, 2011). As noted by some scholars, however, this is not always plausible. Some risks are simply unknown or too complex to be targeted by such an approach (Cavusoglu et al., 2008; Sun et al., 2006). Intent may be clearly expressed in terms of maintaining organisational efficiency, but knowing how to achieve the desired outcome is not always as clear as

simply weighing risks with respect to costs and benefits when such insights might not exist or be known.

Similar challenges were also found in the *capability to adapt security controls to enable resources and integrate/reconfigure beliefs held by various stakeholders*. Implementing adequate controls is often seen as a natural reflection of a risk's priority. However, the capability to *understand adequate controls* illustrates the difficulty of aligning intent with knowledge. For example, intentions may be clear after risks are prioritised, but knowing what accounts for adequate controls and how to implement them is not always as clear. This misalignment can be seen in Njenga and Brown's (2012) study in which the actual risk practice was shaped by the practitioner's knowledge through experience. The study showed how practitioners intended to preserve security, but they exercised their knowledge to make sense of the requested system changes, shaping the practice and its outcome. Njenga and Brown's (2012) case is interesting as it demonstrates that capability is an ongoing accomplishment that is constructed and reconstructed through the work of practitioners (Orlikowski, 2002).

Misalignment between intent and knowledge can also be seen in *integrating beliefs and held values*. Implemented security controls not aligned with the intent to use them can cause controls to become only spontaneously applied in response to individuals' own motivation (Tsohou et al., 2015). If people do not believe or recognise value in the controls being implemented, why would they intend to comply? The challenge of the intent to comply was also seen in the *capability to sustain the integrated resources and competences of stakeholders to continue the alignment with the intended outcome.* For example, literature on the capability of *preserving compliance* outlined various suggestions for creating and maintaining the intent to stay compliant with implemented controls. Some scholars suggest that intent can be motivated by fear of being prosecuted for misbehaviour (Straub and Welke, 1998); others suggested producing a feeling of being personally responsible (Spears and Barki, 2010). The intent to comply and the knowledge about security controls could lead to the capability of maintaining *risk reduction awareness.* The capability of risk reduction is driven by individuals' motivation to actively mitigate risks and is arguably the result of knowledge and a strong intent to contribute. This topic is ripe for further research, which could investigate how intent and knowledge can be attained over time and embedded into routines (Levitt and March, 1988; March, 1991).

6 Conclusions

This literature review contributes to the discussion on ISRM by studying what capabilities are embedded in its routines. Based on four general routine practices (identify, prioritise, implement and control), this review analysed literature on ISRM from a practice-based perspective. A theoretical framework was developed, framing capabilities as knowing how to adapt, integrate and reconfigure skills, resources and competences to achieve intended future conditions. The resulting literature highlighted four capabilities within routine practices, namely the capabilities of integrating various perspectives and values to reach a risk perception aligned with the intended outcome (identify); adapting to varying perspectives of risks and prioritising them in accordance with the intended outcome (prioritise); adapting security controls to enable resources, and integrate/reconfigure beliefs held by various stakeholders (implement); and sustaining the

integrated resources and competences held by stakeholders to continue the alignment with the intended outcome (monitor). Future research should build on the practice-based perspective, studying ISRM in relation to intent and knowing and how these capabilities can be developed in practice.

Acknowledgements

Financing for the CYNIC project (20201650) from the EU program INTERREG North 2014–2020 which supports cross-border collaboration to strengthen competitiveness and attractiveness in and between northern Sweden, northern Finland, northern Norway and Sápmi, and Region Norrbotten and Lapin Liitto are gratefully acknowledged.

References

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

Bandyopadhyay, K., Mykytyn, P.P. and Mykytyn, K. (1999) 'A framework for integrated risk management in information technology', *Management Decision*, Vol. 37, No. 5, pp.437–445.

Baskerville, R. (1991) 'Risk analysis: an interpretive feasibility tool in justifying information systems security', *European Journal of Information Systems*, Vol. 1, No. 2, pp.121–130.

Baskerville, R. (2005) 'Best practices in it risk management: buying safeguards, designing security architecture, or managing information risk', *Cutter Benchmark Review*, Vol. 5, No. 12, pp.5–12.

Berente, N., Lyytinen, K., Yoo, Y. and King, J.L. 2016) 'Routines as shock absorbers during organizational transformation: integration, control, and NASA's enterprise information system', *Organization Science*.

Birch, D.G. and McEvoy, N.A. 1992) 'Risk analysis for information systems', *Journal of Information Technology*, Vol. 7, No. 1, pp.44–53.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. 2010) 'Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness', *MIS Q.*, Vol. 34, No. 3, pp.523–548.

Carlile, P.R. 2002) 'A pragmatic view of knowledge and boundaries: boundary objects in new product development', *Organization Science*, Vol. 13, No. 4, pp.442–455.

Cavusoglu, H., Raghunathan, S. and Yue, W.T. 2008) 'Decision-theoretic and game-theoretic approaches to it security investment', *Journal of Management Information Systems*, Vol. 25, No. 2, pp.281–304.

Chen, P-Y., Kataria, G. and Krishnan, R. (2011) 'Correlated failures, diversification, and information security risk management', *MIS Q.*, Vol. 35, No. 2, pp.397–422.

Chen, Y., Ramamurthy, K. and Wen, K.-W. (2012) 'Organizations' information security policy compliance: stick or carrot approach?', *Journal of Management Information Systems*, Vol. 29, No. 3, pp.157–188.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R. (2013) 'Future directions for behavioral information security research', *Computers& Security*, No. 32, pp.90–101.

Culnan, M.J. and Williams, C.C. 2009) 'How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches', *Mis Quarterly*, Vol. 33, No. 4, pp.673–687.

Dhillon, G. and Backhouse, J. 2000) 'Technical opinion: information system security management in the new millennium', *Commun. ACM*, Vol. 43, No. 7, pp.125–128.

Dhillon, G. and Backhouse, J. 2001) 'Current directions in IS security research: towards socio-organizational perspectives', *Information Systems Journal*, Vol. 11, No. 2, pp.127–153.

Dhillon, G. and Torkzadeh, G. (2006) 'Value-focused assessment of information system security in organizations', *Information Systems Journal*, Vol. 16, No. 3, pp.293–314.

Dixon-Woods, M., Bonas, S., Booth, A., Jones, D.R., Miller, T., Sutton, A.J., Shaw, R.L., Smith, J.A. and Young, B. (2006) 'How can systematic reviews incorporate qualitative research? A critical perspective', *Qualitative Research*, Vol. 6, No. 1, pp.27–44.

Ernst & Young (2012) *Global Information Security Survey 2012: Fighting to Close the Gap*, EYGM Limited, EYG No. AU1889.

Feldman, M.S. and Pentland, B.T. (2003) 'Reconceptualizing organizational routines as a source of flexibility and change', *Administrative Science Quarterly*, Vol. 48, No. 1, p.94.

Feldman, M.S., Pentland, B.T., D'Adderio, L. and Lazaric, N. (2016) 'Beyond routines as things: introduction to the special issue on routine dynamics', *Organization Science*, Vol. 27, No. 3, pp.505–513.

Galbreth, M.R. and Shor, M. (2010) 'The impact of malicious agents on the enterprise software industry', *MIS Quarterly*, Vol. 34, No. 3, pp.595–612.

Goldstein, J., Chernobai, A. and Benaroch, M. (2011) 'An event study analysis of the economic impact of IT operational risk and its subcategories', *Journal of the Association for Information Systems*, Vol. 12, No. 9, p.606.

Halliday, S., Badenhorst, K. and von Solms, R. (1996) 'A business approach to effective information technology risk analysis and management', *Information Management & Computer Security*, Vol. 4, No. 1, pp.19–31.

Herath, T. and Rao, H.R. (2009) 'Protection motivation and deterrence: a framework for security policy compliance in organisations', *European Journal of Information Systems*, Vol. 18, No. 2, pp.106–125.

Hirsch, C. and Ezingeard, J-N. (2008) 'Perceptual and cultural aspects of risk management alignment: a case Study', *Journal of Information System Security*, Vol. 4, No. 1, pp.3–20.

Hsu, C., Backhouse, J. and Silva, L. (2014) 'Institutionalizing operational risk management: an empirical study', *Journal of Information Technology*, Vol. 29, No. 1, pp.59–72.

Hsu, C.W. (2009) 'Frame misalignment: interpreting the implementation of information systems security certification in an organization', *European Journal of Information Systems*, Vol. 18, No. 2, pp.140–150.

ISO/IEC 27005 (2013) *ISO/IEC 27005: Information Technology-Security Techniques -Information Security Risk Management*, ISO, Geneva.

Johnson, P. and Johansson, E. (2008) 'Assessment of business process information security', *International Journal of Business Process Integration and Management*, Vol. 3, No. 2, p.118.

Kitchenham, B. (2004) *Procedures for Performing Systematic Reviews*, Joint Technical Report, Computer Science Department, Keele University and National ICT Australia Ltd.

Kornberger, M. and Clegg, S. (2011) 'Strategy as performative practice: the case of Sydney 2030', *Strategic Organization*, Vol. 9, No. 2, pp.136–162.

Kumar, R.L., Park, S. and Subramaniam, C. (2008) 'Understanding the value of countermeasure portfolios in information systems security', *Journal of Management Information Systems*, Vol. 25, No. 2, pp.241–280.

Kwon, J. and Johnson, M.E. (2013) 'Health-care security strategies for data protection and regulatory compliance', *Journal of Management Information Systems*, Vol. 30, No. 2, pp.41–66 [online] https://doi.org/10.2753/MIS0742-1222300202.

Levitt, B. and March, J.G. (1988) 'Organizational learning', *Annual Review of Sociology*, Vol. 14, No. 1, pp.319–338.

Li, H., Sarathy, R., Zhang, J. and Luo, X. (2014) 'Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance: determinants of IUP compliance', *Information Systems Journal*, Vol. 24, No. 6, pp.479–502.

Lowry, P.B. and Moody, G.D. (2015) 'Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies: proposing the control-reactance compliance model (CRCM)', *Information Systems Journal*, Vol. 25, No. 5, pp.433–463.

Lowry, P.B., Posey, C., Bennett, R.B.J. and Roberts, T.L. (2015) 'Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust: using fairness and reactance theories to decrease reactive computer abuse', *Information Systems Journal*, Vol. 25, No. 3, pp.193–273.

Malle, B.F. and Knobe, J. (1997) 'The folk concept of intentionality', *Journal of Experimental Social Psychology*, Vol. 33, No. 2, pp.101–121.

March, J.G. (1991) 'Exploration and exploitation in organizational learning', *Organization Science*, Vol. 2, No. 1, pp.71–87.

McAdams, A.C. (2004) 'Security and risk management: a fundamental business issue', *Information Management*, Vol. 38, No. 4, p.36.

NIST, J.T.F.T. (2011) *Managing Information Security Risk: Organization, Mission, and Information System View*, No. NIST SP 800-39, Gaithersburg, MD, National Institute of Standards & Technology, USA.

Njenga, K. and Brown, I. (2012) 'Conceptualising improvisation in information systems security', *European Journal of Information Systems*, Vol. 21, No. 6, pp.592–607.

Oetzel, M.C. and Spiekermann, S. (2014) 'A systematic methodology for privacy impact assessments: a design science approach', *European Journal of Information Systems*, Vol. 23, No. 2, pp.126–150.

Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T. and Kagaya, T. (2009) 'Information security governance framework', *Proceedings of the First ACM Workshop on Information Security Governance, WISG '09*, ACM, New York, NY, USA, pp.1–6.

Okoli, C. and Schabram, K. (2010) *A Guide to Conducting a Systematic Literature Review of Information Systems Research*, Sprouts: Working Papers on Information Systems (10: 26).

Orlikowski, W.J. (2002) 'Knowing in practice: enacting a collective capability in distributed organizing', *Organization Science*, Vol. 13, No. 3, pp.249–273.

Padyab, A.M., Päivärinta, T. and Harnesk, D. (2014) 'Genre-based approach to assessing information and knowledge security risks', *International Journal of Knowledge Management*, Vol. 10, No. 2, pp.13–27.

Posey, C., Bennett, R.J. and Roberts, T.L. (2011) 'Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes', *Computers & Security*, Vol. 30, Nos. 6–7, pp.486–497.

Rainer Jr., R.K., Snyder, C.A. and Carr, H.H. (1991) 'Risk analysis for information technology', *Journal of Management Information Systems*, Vol. 8, No. 1, pp.129–147.

Ritchie, J. and Spencer, L. (2002) 'qualitative data analysis for applied policy research', in *The Qualitative Researcher's Companion*, pp.173–194, Sage Publications, Thousand Oaks, CA.

Shamala, P., Ahmad, R., Zolait, A.H. and bin Sahib, S. (2015) 'Collective information structure model for information security risk assessment (ISRA) ', *Journal of Systems and Information Technology*, Vol. 17, No. 2, pp.193–219.

Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. (2016) 'Taxonomy of information security risk assessment (ISRA)', *Computers & Security*, No. 57, pp.14–30.

Shedden, P., Ruighaver, T. and Ahmad, A. (2010) 'Risk management standards – the perception of ease of use', *Journal of Information System Security*, Vol. 6, No. 3, pp.23–41.

Shedden, P., Scheepers, R., Smith, W. and Ahmad, A. (2011) 'Incorporating a knowledge perspective into security risk assessments', *Journal of Information and Knowledge Management Systems*, Vol. 41, No. 2, pp.152–166.

Siponen, M. (2002) 'A paradigmatic analysis of conventional approaches for developing and managing secure IS', in Dupuy, M. and Paradinas, P. (Eds.): *Trusted Information*, Vol. 65, pp.437–452, Kluwer Academic Publishers, Boston.

Siponen, M. (2006) 'Information security standards focus on the existence of process, not its content', *Communications of the ACM*, Vol. 49, No. 8, p.97.

Siponen, M.T. (2000a) 'A conceptual foundation for organizational information security awareness', *Information Management & Computer Security*, Vol. 8, No. 1, pp.31–41.

Siponen, M.T. (2000b) 'Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice', *Information Management & Computer Security*, Vol. 8, No. 5, pp.197–209.

Smith, S., Winchester, D., Bunker, D. and Jamieson, R. (2010) 'Circuits of power: a study of mandated compliance to an information systems security' De Jure' standard in a government organization', *MIS Quarterly*, Vol. 34, No. 4, pp.463–486.

Spagnoletti, P. and Resca, A. (2008) 'The duality of information security management: fighting against predictable and unpredictable threats', *Journal of Information System Security*, Vol. 4, No. 3, pp.46–62.

Spears, J.L. (2006) 'A holistic risk analysis method for identifying information security risks', in Dowland, P., Furnell, S., Thuraisingham, B. and Wang, X.S. (Eds.): *Security Management, Integrity, and Internal Control in Information Systems: IFIP TC-11 WG 11.1 & WG 11.5 Joint Working Conference*, pp.185–202.

Spears, J.L. and Barki, H. (2010) 'User participation in information systems security risk management', *MIS Q.*, Vol. 34, No. 3, pp.503–522.

Straub, D.W. and Welke, R.J. (1998) 'Coping with systems risk: security planning models for management decision making', *MIS Quarterly*, Vol. 22, No. 4, pp.441–469.

Sun, L., Ivastava, R.P. and Mock, T.J. (2006) 'An information systems security risk assessment model under the Dempster-Shafer theory of belief functions', *Journal of Management Information Systems*, Vol. 22, No. 4, pp.109–142.

Sutton, S.G., Khazanchi, D., Hampton, C. and Arnold, V. (2008) 'Risk analysis in extended enterprise environments: identification of critical risk factors in B2B e-commerce relationships', *Journal of the Association for Information Systems*, Vol. 9, Nos. 3–4, pp.151–174.

Taylor, R.G. and Brice, J. (2012) 'Fact or fiction? A study of managerial perceptions applied to an analysis of organizational security risk', *Journal of Organizational Culture, Communications and Conflict*, Vol. 16, No. 1, pp.1–23.

Teece, D.J., Pisano, G. and Shuen, A. 1997) 'Dynamic capabilities and strategic management', *Strategic Management Journal*, Vol. 18, No. 7, pp.509–533 [online] https://doi.org/10.1002/(SICI)1097-0266(199708)18:7<509::AID-SMJ882>3.0.CO;2-Z.

Tranfield, D., Denyer, D. and Smart, P. (2003) 'Towards a methodology for developing evidence-informed management knowledge by means of systematic review', *British Journal of Management*, Vol. 14, No. 3, pp.207–222.

Tsohou, A., Karyda, M., Kokolakis, S. and Kiountouzis, E. (2015) 'Managing the introduction of information security awareness programmes in organisations', *European Journal of Information Systems*, Vol. 24, No. 1, pp.38–58.

Veiga, A.D. and Eloff, J.H.P. (2010) 'A Framework and assessment instrument for information security culture', *Computers & Security*, Vol. 29, No. 2, pp.196–207.

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

Visintine, V. (2003) *An Introduction to Information Risk Assessment*, SANS Institute, No. 8, Maryland, USA.

Von Krogh, G., Ichijō, K. and Nonaka, I. (2000) *Enabling Knowledge Creation: How to Unlock the Mystery of Tacit Knowledge and Release the Power of Innovation*, Oxford University Press, Oxford; New York.

Warkentin, M. and Willison, R. (2009) 'Behavioral and policy issues in information systems security: the insider threat', *European Journal of Information Systems*, Vol. 18, No. 2, p.101.

Webb, J., Ahmad, A., Maynard, S. and Shanks, G. (2016) 'Foundations for an intelligence-driven information security risk-management system', *Journal of Information Technology Theory and Application (JITTA)*, Vol. 17, No. 3, p.3.

Webster, J. and Watson, R.T. (2002) 'Analyzing the past to prepare for the future: writing a literature review', *MIS Quarterly*, Vol. 26, No. 2, pp.13–23.

Werlinger, R., Muldner, K., Hawkey, K. and Beznosov, K. (2010) 'Preparation, detection, and analysis: the diagnostic work of IT security incident response', in Furnell, M. (Eds.): *Information Management & Computer Security*, Vol. 18, No. 1, pp.26–42.

Whitman, M.E. and Mattord, H.J. (2014) *Management of Information Security*, 4th ed., Cengage Learning, Stamford, CT, USA.

Whittington, R. (2006) 'Completing the practice turn in strategy research', *Organization Studies*, Vol. 27, No. 5, pp.613–634.

Wolff, J. (2016) 'Perverse effects in defense of computer systems: when more is less', *Journal of Management Information Systems*, Vol. 33, No. 2, pp.597–620.

Zhao, X., Xue, L. and Whinston, A. B. (2013) 'Managing interdependent information security risks: cyberinsurance, managed security services, and risk pooling arrangements', *Journal of Management Information Systems*, Vol. 30, No. 1, pp.123–152.

Notes

1 http://aisnet.org/?SeniorScholarBasket.

2 The citation looks for an exact match; AND and OR are Boolean operators.

Paper B

Dynamic interplay in the information security risk management process

Lundgren, M. and Bergström, E. (2019) 'Dynamic interplay in the information security risk management process,' *Int. J. Risk Assessment and Management*, Vol. 22, No. 2, pp.212–230.

Dynamic interplay in the information security risk management process

Martin Lundgren*

Department of Computer Science,
Luleå University of Technology, Sweden
Email: Martin.Lundgren@ltu.se
*Corresponding author

Erik Bergström

School of Informatics,
University of Skövde, Sweden
Email: Erik.Bergstrom@his.se

Abstract: In this paper, the formal processes so often assumed in information security risk management and its activities are investigated. For instance, information classification, risk analysis, and security controls are often presented in a predominantly instrumental progression. This approach, however, has received scholarly criticism, as it omits social and organisational aspects, creating a gap between formal and actual processes. This study argues that there is an incomplete understanding of how the activities within these processes actually interplay in practice. For this study, senior information security managers from four major Swedish government agencies were interviewed. As a result, 12 characteristics are presented that reflect an interplay between activities and that have implications for research, as well as for developers of standards and guidelines. The study's conclusions suggest that the information security risk management process should be seen more as an emerging process, where each activity interplays dynamically in response to new requirements and organisational and social challenges.

Keywords: information classification; risk analysis; security controls; interplay; formal processes.

Reference to this paper should be made as follows: Lundgren, M. and Bergström, E. (2019) 'Dynamic interplay in the information security risk management process', *Int. J. Risk Assessment and Management*, Vol. 22, No. 2, pp.212–230.

Biographical notes: Martin Lundgren is a PhD candidate in Information Systems at Luleå University of Technology, Sweden. He received his BSc in Informatics from University of Gothenburg Sweden in 2012, and his MSc in Information Security from Luleå University of Technology in 2014. His general research interests are information security and risk management from socio-organisational perspectives.

Erik Bergström is a doctoral candidate at the School of Informatics at the University of Skövde, Sweden. His main research interest lies in the field of information security management with a focus on information classification practices.

1 Introduction

Information security risk management (ISRM) can be defined as protecting and preserving the confidentiality, integrity, and availability of information (ISO/IEC 27001, 2013; Whitman and Mattord, 2014). ISRM has seen the development of several processes that vary in specific steps and procedures but typically include activities for identifying and valuing information assets, risks and implementing and monitoring security controls (ISO/IEC 27005, 2013; Shedden et al., 2010; Visintine, 2003; Whitman and Mattord, 2014). Information classification is an activity where information is valued with respect to the loss of confidentiality, integrity, and availability, for example (Breier and Schindler, 2014; Fowler, 2003), and it is a prerequisite for analysing risks (ISO/IEC 27002, 2013). In information security, risk is commonly referred to as the potential that a given threat will be exploited and the harm it could cause the organisation (ISO/IEC 27001, 2013; Lo and Chen, 2012). Identifying and prioritising risk, referred to here as risk analysis, is the activity concerned with balancing the value of the information assets identified for protection against recognised threats and is a prerequisite for selecting possible security controls to mitigate or accept the known risks (Eloff et al., 1993; Fowler, 2003; Gerber and von Solms, 2005). Security controls can be any "process, policy, procedure, guideline, practice or organizational structure, which can be administrative, technical, management, or legal in nature which modifies information security risk" [ISO/IEC 27005, (2013), p.2]. The literature often depicts information classification, risk analysis, and security controls as activities performed in a predominantly instrumental fashion: where information classification serves as input for a risk analysis that leads to a rational decision regarding security controls, followed by a feedback operation (ISO/IEC 27001, 2013; Straub and Welke, 1998).

Over the past decades, a substantial body of literature has evolved on the importance and role of ISRM and its activities, but there has been less focus on how it is practised. However, whilst several scholars have recognised this gap between formal processes and those used in practice (Alaskar et al., 2015; Niemimaa and Niemimaa, 2017; Njenga and Brown, 2012; Shedden et al., 2010; Siponen, 2006; Taylor, 2006; Taylor and Brice, 2012), the relationship between the activities and their interplay, i.e., how activities affect each other in practice (Coles-Kemp, 2009), has received limited attention. Considering that information classification, risk analysis, and security controls may be split up and conducted in parallel or in a different order when appropriate (Parker, 2007), the organisational and social challenges that 'lie between' each activity could reveal clues about what needs to be investigated. Nevertheless, such 'in-between' studies are rare, but there are indications that they are needed. For example, Ozkan and Karabacak (2010) conclude that it is not always evident what information needs to be classified and how to classify it before conducting the risk analysis. This problem has been described by Sajko et al. (2006) as one of the main difficulties in assessing risk analysis. When viewing information classification, risk analysis and security controls as activities in an ISRM process, it is not evident what happens when adapting to new requirements or what constitutes adequate security controls in relation to information classification and risk analysis (Baskerville, 1991; Taylor, 2015). Over time, several researchers have stressed that research needs to address such challenges to better understand the organisational and social aspects of ISRM (Coles-Kemp, 2009; Sajko et al., 2006; Tatar and Karabacak,

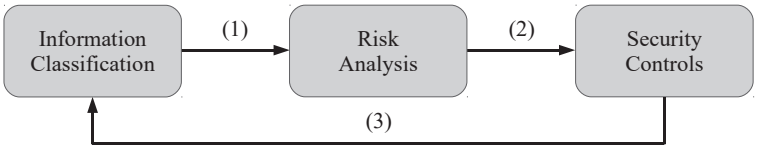
2012). Thus, this paper aims to analyse the interplay between information classification, risk analysis, and security controls in practice.

This paper is organised as follows: the following section discusses a challenge-based perspective, followed by Section 3, which presents the study design. Section 4 presents the findings, and Section 5 highlights the study's contributions and discusses its implications and recommendations for future research.

2 A rational outlook on the risk management process

As problematised above, information classification, risk analysis, and security controls are often visualised as a series of activities (see Figure 1). After all, this approach provides a rational process, which has been widely described and adopted in research and standards alike. For example, Straub and Welke (1998), Reid and Floyd (2001) and Spears and Barki (2010) outline continuous processes for identifying and prioritising information assets and security risks, to implementing and monitoring security controls, followed by a feedback operation to be repeated, if necessary. Similarly, recognised standards such as the ISO 27000 series recommend a similar set of activities, often outlined as a lifecycle: "a) identify information assets b) assess information security risks […] c) select and implement relevant controls […] d) monitor, maintain and improve" [ISO/IEC 27000, (2014), p.15].

Figure 1 A general ISRM process, as described in both research and standards



In an approach such as the one outlined above, each activity's output serves as a necessary input for the next activity. For example, estimating a risk's impact is often expressed as a formula based on vulnerability, likelihood and how critical the information asset is to the organisation. Hence, a critical step before risk analysis is the output from the information classification (Figure 1, step 1) resulting in an information asset valuation (ISO/IEC 27002, 2013; Whitman and Mattord, 2014). Likewise, the purpose of security controls is to respond to risks, but in order to make a rational decision regarding what risks to mitigate and what risks to accept, the output from the risk analysis (Figure 1, step 2) in the form of an inventory of identified risks and their level of impact is required (Shameli-Sendi et al., 2016; Whitman and Mattord, 2014). In addition, many processes outline a feedback operation to convey historical data from the security controls such as incidents (Figure 1, step 3), to continuously improve and ensure that they provide an appropriate level of protection for the organisation's information assets, and remain relevant for new risks over time (Ahmad et al., 2012; Webb et al., 2014).

Such an approach advocates instrumental relationships between the activities of information classification, risk analysis, and security control selection and implementation. Whilst providing valuable insight regarding implementation, it primarily

describes ideal inputs and outputs that should ultimately lead to adequate security controls that address the requirements of confidentiality, integrity, and availability (Dhillon and Backhouse, 2000). To this end, formal process models serve as rational guidance for activities, to prevent them from being performed on an ad hoc basis (Ashenden, 2008; Parnas and Clements, 1986). However, the actual processes are shaped within the enactment of day-to-day activities and their respective challenges (Feldman, 2000). Consequently, the formal process gives rise to the perception that the activities are static and not dynamic. This instrumental conceptualisation of ISRM has previously received scholarly criticism as it assumes there will be controllable and predictable solutions to protect assets but fails to address the important social and organisational dimensions (Dhillon and Backhouse, 2000; Dhillon and Torkzadeh, 2006; Doherty et al., 2009). Socially constructed concepts such as values, beliefs and perceptions of security and information assets, and organisational influences such as the use of technology, organisational purpose and agility, can change the relationship between an ISRM process and its users by influencing its activities (Coles-Kemp, 2009).

Omitting such social and organisational aspects can lead to difficulties in handling uncertainties or surprises (Ciborra, 1996; Njenga and Brown, 2012) and remain inflexible in the face of changing requirements driven by the complexity and uncertainty of real-life situations. Because of this inflexibility, ISRM processes will continue to represent an ideal for several reasons (Parnas and Clements, 1986). First, managers and information owners seldom know what assets to protect (Ku et al., 2009; Sajko et al., 2006) or how to integrate different perspectives on the value of information (Dhillon and Torkzadeh, 2006). Second, even if all information assets were known, some details and circumstances will not be discovered until later, such as changes in the value of information as a part of its information lifecycle. Likewise, there is a need to adapt to different desired outcomes based on varying requirements (Hsu, 2009; Tsohou et al., 2015), such as balancing cost and security restrictions with the information value (Goldstein et al., 2011; Kumar et al., 2008). Even if all details and circumstances are known, humans can only manage so much complexity. Lastly, even if such complexity could be managed, external forces can lead to changes in requirements that may invalidate earlier decisions. For example, adapting to new threats, laws or requirements to remain compliant (Kwon and Johnson, 2013; Lowry and Moody, 2015), or how the roles of power and politics affect the very standardisation of such compliance requirements (Backhouse et al., 2006). Understanding such challenges provides details about the process and can be used as an analytical lens to examine ISRM activities and how they interplay in actual practice.

3 Study design

To analyse how information classification, risk analysis, and security controls interplay in practice, an interpretive approach was utilised in which qualitative data was obtained (Braa and Vidgen, 1999). The method applied a qualitative content analysis using an inductive approach, which is appropriate when investigating phenomenon with limited or fragmented knowledge (Elo and Kyngäs, 2008).

3.1 Interview guide

In preparation for the interviews, a semi-structured interview guide was created. To capture social and organisational challenges within ISRM, the interview guide drew from Lundgren's (forthcoming) review on risk challenges within information security. These eight identified challenges were complemented with additional sources to include challenges within information classification and to provide an analytical lens to examine the social and organisational perspectives, as discussed in section two. These challenges were used as the basis for developing the interview questions. The interview questions were developed to be focused but not leading, to avoid imposing perceptions or lead the interviewee to assume particular relationships between activities. Hence, questions directly targeting activity relationships were avoided. Instead, open-ended question targeting activities, practices, and processes as a whole were asked to gain insight into their underlying motivations and the reasons for activity relationships when moving between activities. The following eight challenges along with sample questions are listed below:

- Integrating different perceptions – The relative desirability of consequence in security function or purpose (e.g., Dhillon and Torkzadeh, 2006; Lowry and Moody, 2015). Questions developed for this challenge included "In your experience and from what you may have noticed, are there any varying perceptions on security controls? If so, could you explain the origin and/or motivation for these perceptions?"
- Integrating different information value – The subjective judgement of information value existing within individual perception, motivating what enables or constrains a certain practice (e.g., Kaarst-Brown and Thompson, 2015; Oetzel and Spiekermann, 2014). Questions developed for this challenge included "Could you describe what it means for you to perform information classification? Could there ever be situations where it is not possible to classify the information in alignment with organizational guidelines?"
- Adapting to different desired outcomes – The different expectations that may result from varying competences and priorities in day-to-day work (e.g., Hsu, 2009; Sutton et al., 2008). Questions developed for this challenge included "To your knowledge, have there ever been situations where implemented security controls do not align well with other day-to-day work in your organization?"
- Knowing the balance between security and value – The balance between the value of the information that is to be protected, and the security costs and restrictions this may imply (e.g., Galbreth and Shor, 2010; Puhakainen and Siponen, 2010). Questions developed for this challenge included "In your experience, can there be challenges when balancing security controls against asset values? For example, how would you resolve a situation where asset value is considered lower than the cost of a recommended security control?"
- Understanding adequate controls – To adequately balance the relative subjectivity in information value and risk perception (e.g., Njenga and Brown, 2012; Spears and Barki, 2010). Questions developed for this challenge included "Could you describe how you arrive at a recommended security control? Does asset value and perceived security risk affect the selection of security controls?"

- Integrating beliefs and held values – Factors such as competence, culture, and beliefs that can cause security procedures to be viewed as justified and that motivate compliance (e.g., Hepsø et al., 2009; Tsohou et al., 2015). Questions developed for this challenge included "How does your organization encourage employees to follow your internal guidelines?"
- Preserving compliance – Commitment to information value and motivate compliance with established security procedures in day-to-day work (e.g., Chen et al., 2012; Niemimaa and Niemimaa, 2017). Questions developed for this challenge included "How does your organization view education on ISRM activities in day-to-day work? In your own words, how would you describe the overall commitment to and motivation for complying with your ISRM process?"
- Alertness in adapting to new configurations – Adjusting to new information realities, risks and vigilance towards security procedures. It is the difference between stagnated compliance and evolving security (e.g., Culnan and Williams, 2009; Kwon and Johnson, 2013). Questions developed for this challenge included "How does your organization work internally to keep your ISRM process relevant over time? For example, what could cause the need for a reclassification of information assets?"

The complete interview guide was subjected to a pilot interview conducted with a representative from a Swedish government agency who did not participate in the actual study. The questions were then refined and revised based on the questions and suggestions, and the final interview guide contained a total of about 30 questions.

3.2 Sample and data collection

It is considered difficult to obtain field data on how ISRM processes are enacted in practice (Baskerville et al., 2018; Kotulic and Clark, 2004). Considering that this study aims to capture social and organisational challenges that 'lie between' each activity within the ISRM process, in-depth data was sought to capture these dynamics. Therefore, insight into how such processes are practised within an organisation would preferably not solely depend on interviews (Kotulic and Clark, 2004) but also on an understanding of the background of rules and expectations, such as internal guidelines; this would provide richer insight into the ostensible practice, as well as the actual practice of ISRM activities (Feldman and Pentland, 2003).

In this study, we targeted Swedish government agencies for two main reasons.

1 Swedish government agencies are autonomous, especially in comparison with other countries, which has some consequences regarding ISRM. For example, all government agencies are mandated to systematically conduct ISRM, but no standardised process is enforced, which has led to a wide range of adopted practices.

2 The principle of public access to official records, in most cases, enables access to the internal guidelines of these agencies.

Despite the mandate described above, not all agencies have implemented an ISRM process (Swedish Civil Contingencies Agency, 2014), which limits the selection of study objects. The final selection of agencies was based on a previous study (Bergström et al., 2018) in which four agencies demonstrated mature ISRM processes, including formal

guidelines and well-described practices. Furthermore, the four agencies were also selected because they operate in different sectors that provide services and data critical to society (see 'Sector and mission' in Table 1). Considering their critical role to society, destruction or disruption of their information systems could affect national capabilities such as emergency response, for example. Thus, ISRM is crucial in their respective organisations.

Table 1 Background details on the organisations and interviewees

ID	*Sector and mission*	*Employees*	*Role(s)*
A1	Enterprise and innovation. Supplies e.g., geodata critical to society in emergency situations.	~2,000	Information Security Coordinator, and IT Architect
A2	Health and social affairs. Handles e.g., economic transactions within one part of the Swedish welfare system.	~1,200	Security Specialist
A3	Environment and energy. Handles e.g., warning services for the public.	~650	Security Architect
A4	Public sector coordination. Handles e.g., cross-sectoral issues related to disaster and emergency preparedness, and civil defence.	~230	Director of Preparedness and Response

Interviews were conducted with representatives from four major Swedish government agencies, hereafter referred to as A1–A4. In total, five senior information security managers involved in their respective ISRM processes were interviewed. For all agencies but A1, the interviews were conducted individually. In A1's case, a group interview was conducted since they had shared responsibilities.

Before the interviews, a short reminder e-mail was sent to each interview subject, describing the objective of the research and introducing two questions to be considered before the interview. The first question asked if the subject could recall any particularly successful ISRM process (information classification, risk analysis, and security controls), and what factors they thought were key to its success. The second question presented three scenarios in which requirements regarding information classification, risk analysis, and security controls were suddenly altered, and if/how the subject thought that would affect their ISRM process.

The four interviews were recorded and lasted 50–90 minutes each. The researchers took turns taking notes (as backup) and acting as the interview leader. Directly after each interview, a contact summary was filled out by both researchers individually, as suggested by Huberman and Miles (2002). The contact summary was designed to capture the most salient points of the interview, whilst still fresh in mind, including issues and impressions. The recordings were then divided among the two authors and transcribed, each correcting the other's transcription. The transcribed text amounted to 52 pages.

3.3 Data analysis

Before the data analysis, codes were agreed upon. The codes derived from the unidirectional relationship between every combination of the activities for information classification, risk analysis, and security controls. This was done in order to cover all

possible relationships between the ISRM activities, considering that the aim of this study was to capture the interplay between each activity. This resulted in a total of six codes:

- information classification → risk analysis
- risk analysis → information classification
- risk analysis → security controls
- security controls → risk analysis
- security controls → information classification
- information classification → security controls.

The data analysis was performed in four steps, based on the qualitative content analysis (Cho and Lee, 2014).

1 Each transcript was individually subjected to a concept-driven coding (Ritchie and Spencer, 2002) by the authors, identifying chunks of text that typified any of the six codes. The authors' results were then merged into six separate documents (coding manuals), with each document representing one of the codes.

2 The authors then individually and critically examined the text within each coding manual. This meant identifying points of interest and characteristics by highlighting quotes that related to a particular code. From this point forward, the authors jointly conducted the analysis.

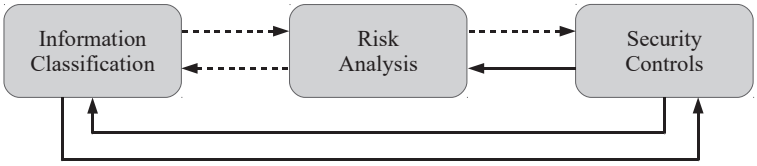
3 The authors iteratively discussed and synthesised the differences and similarities of each coding manual, following the data retrieval process suggested by Gibbs (2007). In practice, differences between the authors were resolved by critically examining the motivation for inclusion and suggested code relationships. For example, discussions about whether a particular quote represented a specific relationship between two ISRM activities were typically situations where consensus needed to be reached. This iterative analysis and comparative discussion made it possible to both frame and re-frame the data to represent each code more in-depth, and to reach consensus among the authors.

4 Each synthesis was then discussed by the authors and developed into relationship characteristics with associated descriptions for each code.

4 Findings

This section presents the results of the synthesised data and is organised by codes as specified in the data analysis. For each code, relationship characteristics identified during the data analysis (12 total) represent the features of the relationship. Figure 2 illustrates the dynamic interplay revealed by the analysis; the solid arrows represent unanimous recognition of the relationship by all agencies, whereas dashed arrows represent differing recognition of the relationship. Under each code section below, a figure illustrating the particular activity relationship is outlined, along with the relationship characteristics and the corresponding agency. A '+' sign indicates whether the relationship characteristic was found for a particular agency, and a '–' sign if not.

Figure 2 The dynamic interplay within the ISRM process, as found in the analysis



4.1 Information classification → risk analysis

Information classification followed by risk analysis is part of a workflow described in many standards. However, it is interesting to note that none of the agencies studied use a full risk analysis as described in most standards (e.g., ISO/IEC 27005, 2013), but rather as a complementary or optional activity. For example, A3 uses risk analysis only for infrastructure systems, and for other systems only if there is something out of the ordinary. The reason is that A3 observed the same risks recurring in the risk analysis. A2's reasoning was similar and resulted in the risk analysis only looking at the risks of not having some of the security controls in place. A3 and A2 both mentioned that it is impossible to keep a dynamic risk analysis alive over time, which directed them to a more static view of the risk analysis. A3 and A2 both referred to risk analysis as static, consisting of a predefined list of threats and vulnerabilities. Another example of the relationship between information classification and risk analysis comes from A1, which did not recognise the need for a risk analysis if the information had a low classification.

Figure 3 The information classification to risk analysis activity with relationship characteristics

Government agency (→)	*A1*	*A2*	*A3*	*A4*
Relationship characteristics (↓)				
Full risk analysis only sometimes required (e.g., information classification is high, and extraordinary situations).	+	+	+	+
Static view of risks in risk analysis (e.g., using predefined lists of threats and vulnerabilities).	–	+	+	–

All of the agencies perceive information classification and risk analysis as two separate events, each performed as a group activity, but partly with different stakeholders. For instance, A1 uses information owners and lawyers in the information classification, whilst for the risk analysis, the focus is on other competencies such as system developers, project managers, and other management roles. Furthermore, A1 explained that it is hard not to think about risks or security controls when performing the information classification, but said so with a tone of regret, implying that it is wrong to do so because

the formal process does not invite such interplay: "when we do classification, people easily say 'this will not happen'. But then you have to intervene and say, 'hold on, we're supposed to only consider consequences, not probability'… these are separate things." The argument is that in classification, only the consequences of a loss (e.g., confidentiality) should be considered and that the classification result could be affected if they start to consider risks that early in the process.

It should be noted that both A1 and A4 argue that a successful risk analysis requires more than just the classification (e.g., a number), and preferably considers more contextual information in the information classification, such as a description of the information and the stakeholders handling the information. This could support the notion suggested by Ozkan and Karabacak (2010) and Sajko et al. (2006) that the information classification to risk analysis relationship is not always straightforward in practice.

4.2 Risk analysis → information classification

The relationship between information classification and risk analysis was the only relationship where a diametrical difference in opinion was shown. On one hand, A3 and A4 both recognised a reciprocal relationship between information classification and risk analysis, arguing that risks can affect the information value. On the other hand, A1 and A2 argued for a strictly unidirectional relationship since risks cannot affect the actual value of the information. However, A1, A3, and A4 expressed difficulty in refraining from reflecting on risks whilst conducting information classification.

Figure 4 The risk analysis to information classification activity with relationship characteristics

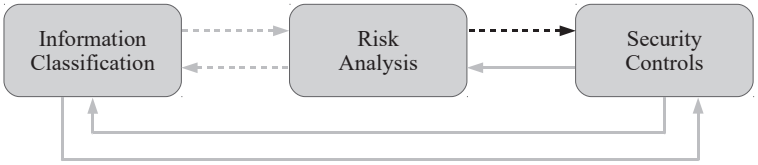
Government agency (→)	*A1*	*A2*	*A3*	*A4*
Relationship characteristics (↓)				
Risk analysis can trigger information classification (thinking of risks can justify information value).	–	–	+	+
Information classification cannot be affected by risk analysis (as risks do not change the information value).	+	+	–	–

This could be interpreted as the result of the challenge in strictly following a formal workflow, as discussed in section two. A3 and A4 promote this relationship by arguing that risk analysis provides information classification with additional insight in selecting a classification level, and hence they argue that there needs to be a reciprocal relationship between the two activities. This relationship can provide additional insight into the challenge of integrating different perceptions (as described by, e.g., Dhillon and Torkzadeh, 2006) into the risk management process.

4.3 Risk analysis → security controls

The analysis showed that risk analysis could add insight and perspectives on what security controls should ultimately be implemented. According to A2, when risk analysis is practised, it ultimately poses the questions of what security controls must be implemented and what risks are acceptable. Or like the control questions suggested by A4: "Should we do something or are existing security controls enough?" Similarly, A1 explains that during information classification, certain information might be classified as high, whilst during risk analysis, second thoughts about the consequences of losing that information may lead to dismissing the implementation of certain security controls. Risk analysis thus acts as the "proof, hint or description of what is important for the board... it justifies what [security controls] to continue with." (A1) As such, A1 and A4 use risk analysis to determine and influence the security controls to implement, whilst A2 addresses risk analysis only to assess deficient security controls and to prioritise the additional security controls needed and the risks to accept.

Figure 5 The risk analysis to security controls activity with relationship characteristics



Government agency (→) / *Relationship characteristics (↓)*	*A1*	*A2*	*A3*	*A4*
Risk analysis acts as a filter between information classification and security controls (e.g., to sift out predetermined security controls).	–	+	–	–
Risk analysis guides the perspectives of what security controls to implement (e.g., what security controls to create or use to accept or mitigate risks).	+	–	–	+

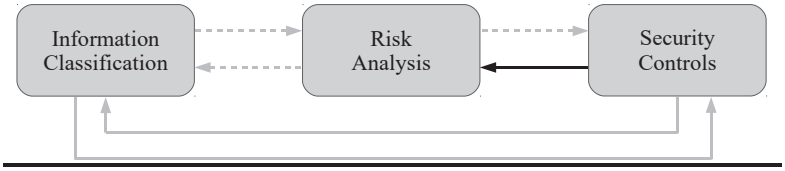
A3 did not, however, express any relationship between risk analysis and security controls, whereas such a relationship is clearly described by the other three agencies and occurred naturally as part of their respective processes. A relationship between the two activities could have a practical implication in better understanding the challenge of maintaining the balance between security and value (as described by Puhakainen and Siponen, 2010). Furthermore, it could also aid in understanding adequate controls (as described by Spears and Barki, 2010), by using risk analysis as a balance between information classification and security controls.

4.4 Security controls → risk analysis

The security controls to risk analysis relationship was illustrated in various cases as a way to adjust planned or already implemented security controls. For example, all agencies described different cases where the actual implementation of security controls became too expensive or complex. In these cases, this can result in returning to the risk analysis

to accept associated risks by omitting the planned security controls (A1), or as A4 described it "one would only need to go back one step [to the risk analysis]: are there any other security controls that could provide a similar result but are not as costly?"

Figure 6 The security controls to risk analysis activity with relationship characteristics



Government agency (→)	*A1*	*A2*	*A3*	*A4*
Relationship characteristics (↓)				
Decided/planned/existing security controls can use risk analysis as a filter (e.g., when security controls are too expensive)	–	+	–	+
Security controls trigger re-evaluation of risk analysis (e.g., when security controls are too expensive or complex or when incidents occur).	+	–	+	+

According to A2 and A4, regarding the relationship between the security controls and risk analysis, planned or already implemented security controls, rather than information classification, serve as an input to the risk analysis to identify possible risks resulting from not having certain security controls in place. For example, in the case presented by A2, security controls are determined before the risk analysis, reducing risk analysis to a kind of filter to determine what risks to accept and what security controls must be implemented. The relationship between the security controls and risk analysis can also be seen when auditing implemented security controls. In this case, security controls are examined if they are still effective and acceptable with regard to the risk analysis (A1). Similarly, the effects of both actual and hypothetical security incidents on security controls are often provided as inputs to the risk analysis activity to evaluate the effectiveness of existing controls or determine the need for the controls (according to A1 and A3).

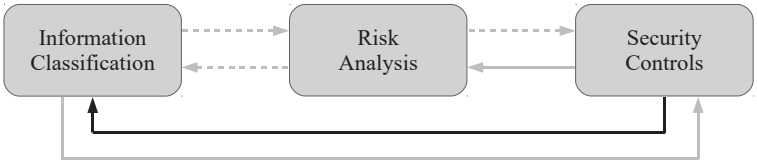
Interestingly, the agencies indicated that new threats do not trigger a re-evaluation of the risk analysis, but external or internal factors regarding security controls such as costs, complexity and incidents do, which means that security controls can trigger a re-evaluation of the risk analysis, which in turn can change the security controls. In other words, there is an interplay that addresses the challenge of alert adoption of new configurations (as described by Culnan and Williams, 2009).

4.5 Security controls → information classification

The progression of security controls to information classification is a part of the flow described in many standards because it often operates as a lifecycle. In other words, this relationship mainly addresses the triggers for a reclassification. All of the agencies use time as a trigger. For example, every two to three years, information is reclassified to update the classifications. External factors such as incidents can also trigger a reclassification because the existing security controls were not up to par and this, in turn,

can trigger a re-evaluation of the asset value. Additionally, both A3 and A2 describe system changes and procurements as a trigger for re-evaluation when new applications or systems are introduced.

Figure 7 The security controls to information classification activity with relationship characteristics



Government agency (→)	*A1*	*A2*	*A3*	*A4*
Relationship characteristics (↓)				
Security controls can help determine information classification levels (e.g., knowledge about security control costs, complexity, etc., can be an input to information classification and balance its value).	+	–	+	–
Security controls trigger reclassification (e.g., time, incidents, changes in requirements, system changes, and procurements).	+	+	+	+

Furthermore, security controls can alter an existing classification level or help determine a classification level. For example, A3 states that once security controls are decided, they might have to go back and change the classification after the planned security controls are discussed with system architects. Similarly, A1 uses an implicit link between security controls and information classification to illustrate the security controls required for a certain classification level. Hence, changes in security controls or in their requirements reflects back on the classification level.

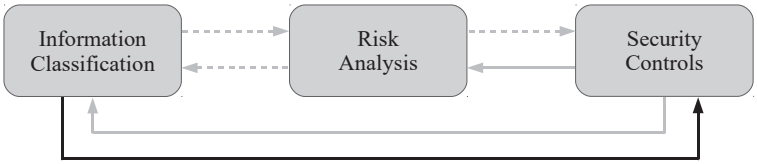
This workflow could help the challenge of integrating different information values, or as A1 described it: to give additional insight in selecting a classification level. This interplay has a practical implication since information classification and security controls could potentially decrease the incidence of subjective judgement in information classification (a common problem described by Kaarst-Brown and Thompson, 2015), as the focus changes from the wording in the classification matrix to security control requirements that could be perceived as being more easily understood. This also connects to the previously described challenge of integrating beliefs and held values.

4.6 Information classification → security controls

The information classification to security controls relationship is not well-documented in the literature, but all of the agencies displayed a direct relationship. For example, A1 states that there is an implicit and unstated relationship in the internal guidelines, but "very often we say… that this information is so important that we impose higher requirements, e.g., on… user credentials or authentication methods" already in the information classification. Similarly, A4 recognises this relationship for information classified at the highest level. In part, the reason behind this is that certain assets, such as personal data, require specific procedures for handling, which are themselves security

controls. A1 also states that the implicit link between information classification and security controls can help people conduct the classification. According to A1, it provides a better understanding of the security controls required for a specific classification level that is not obtained as a consequence of a loss, as otherwise proposed in the literature and standards (ISO/IEC 27000, 2014; Whitman and Mattord, 2014).

Figure 8 The information classification to security controls activity with relationship characteristics



Government agency (→)	*A1*	*A2*	*A3*	*A4*
Relationship characteristics (↓)				
Internal guidelines explicitly specify security controls for all information classification levels.	–	+	+	–
Internal guidelines explicitly specify security controls, but only for specific information types or for the highest classification level.	+	–	–	+

A3 and A2's internal guidelines, on the other hand, have both explicitly described security controls for each level of consequence in their respective information classification scheme. Both agencies see various benefits in this approach. For one, it speeds up the process, since they do not need to start from scratch identifying new security controls every time. Second, it provides a more consistent approach for identifying and implementing security controls in the organisation. However, this circumvents the risk analysis. But in A2's reasoning, this is still a feasible approach because the security controls are taken primarily from ISO 27001. In A2's reasoning, the security controls outlined in the standard carry an inherent risk if they are not implemented, hence there is no need to conduct an additional risk analysis. Furthermore, A2 and A3 also express that the information classification to security controls relationship must exist due to external forces such as legal regulations. For example, the introduction of EU's General Data Protection Regulation (GDPR) will further strengthen the need for a direct relationship between information classification and security controls in order to meet the requirements of demonstrating what and how information is protected.

5 Conclusions

The purpose of this study was to analyse the interplay between information classification, risk analysis, and security controls in actual practice. Representatives from four major Swedish government agencies (A1–A4) have been interviewed, and the study indicates that formal processes, commonly outlined in research and standards as a series of

activities performed in a predetermined order with expected inputs and outputs, do not reflect reality, as actual practice is more dynamic.

Twelve characteristics, as presented in Figures 3–8, have been identified that have both theoretical and practical implications because they indicate social and organisational challenges that affect the process by influencing its activities. For example, organisational factors such as the budget or technological complexity could trigger a re-evaluation of risks to change their outcomes. Similarly, socially constructed concepts such as asset value or beliefs about an activity's outcome could inspire deviations from the formal process to, for example, increase security controls for a particular information asset without conducting a full risk analysis.

However, it was found that not following formal processes can be perceived as something negative. One example of this can be seen in a comparison between A1 and A2, where the former observed any deviation from the formal process (as outlined in many standards and research studies) as something bad, whilst the latter openly embraced such deviations and used them to tailor practices to better fit the context. However, at the same time, the empirical data for all agencies, including A1, indicated that the interplay between activities sparked dialogues that enabled more well-informed decisions, such as choosing a specific information classification level or security control.

In practice, a dynamic interplay emerges between activities, rooted in social and organisational challenges, that ultimately configures the formal process to better fit the given context. In this study, the dynamic interplay was strongest in security controls, as these were often seen as a guide for the valuation of risks or assets. Interestingly, this resulted in a process more driven by security controls than the traditional risk-driven process.

However, future research is recommended to further refine and improve the findings to help visualise the gap between standards and practice and to better describe the interplay in actual practice. To overcome some of the limitations of this study, we recommend more research in both the private and public sectors, within various countries and cultures and using different research designs to further explain the dynamic interplay. Findings from studies that address the fact that processes are practised differently in reality than in theory will have implications for research and for developers of standards and guidelines alike. In practice, this could lead to new instructions for how, when and by whom information classification, risk analysis, and security controls are practised.

Acknowledgements

Financing from the Northern Periphery and Arctic Programme 2014–2020 supported by the European Regional Development Fund (ERDF), Target No. 4, and the European Commission (for funding the Privacy Flag No.653426 project) is gratefully acknowledged.

References

Ahmad, A., Hadgkiss, J. and Ruighaver, A.B. (2012) 'Incident response teams – challenges in supporting the organisational security function', *Computers & Security*, Vol. 31, No. 5, pp.643–652, https://doi.org/10.1016/j.cose.2012.04.001.

Alaskar, M., Vodanovich, S. and Shen, K.N. (2015) 'Evolvement of information security research on employees' behavior: a systematic review and future direction', *48th Hawaii International Conference on System Sciences*, Kauai, HI, January, pp.4241–4250.

Ashenden, D. (2008) 'Information security management: a human challenge?', *Information Security Technical Report*, Vol. 13, No. 4, pp.195–201, https://doi.org/10.1016/j.istr.2008.10.006.

Backhouse, J., Hsu, C.W. and Silva, L. (2006) 'Circuits of power in creating de jure standards: shaping an international information systems security standard', *MIS Q.*, Vol. 30, No. 1, pp.413–438.

Baskerville, R. (1991) 'Risk analysis: an interpretive feasibility tool in justifying information systems security', *European Journal of Information Systems*, Vol. 1, No. 2, pp.121–130.

Baskerville, R., Rowe, F. and Wolff, F-C. (2018) 'Integration of information systems and cybersecurity countermeasures: an exposure to risk perspective', *SIGMIS Database*, Vol. 49, No. 1, pp.33–52, https://doi.org/10.1145/3184444.3184448.

Bergström, E., Åhlfeldt, R-M. and Anteryd, F. (2018) 'Information classification policies: an exploratory investigation', in Dhillon, G. and Samonas, S. (Eds.): Proceedings of the Annual Security Conference, Securing the interconnected world, March, 26-28 2018 Las Vegas, NV.

Braa, K. and Vidgen, R. (1999) 'Interpretation, intervention, and reduction in the organizational laboratory: a framework for in-context information system research', *Accounting, Management and Information Technologies*, Vol. 9, No. 1, pp.25–47, https://doi.org/Doi: 10.1016/s0959-8022(98)00018-6.

Breier, J. and Schindler, F. (2014) 'Assets dependencies model in information security risk management', in *Information and Communication Technology-EurAsia Conference*, Springer, pp.405–412.

Chen, Y., Ramamurthy, K. and Wen, K-W. (2012) 'Organizations' information security policy compliance: stick or carrot approach?', *Journal of Management Information Systems*, Vol. 29, No. 3, pp.157–188, https://doi.org/10.2753/MIS0742-1222290305.

Cho, J.Y. and Lee, E-H. (2014) 'Reducing confusion about grounded theory and qualitative content analysis: similarities and differences', *The Qualitative Report*, Vol. 19, No. 32, p.1.

Ciborra, C.U. (1996) 'The platform organization: recombining strategies, structures, and surprises', *Organization Science*, Vol. 7, No. 2, pp.103–118.

Coles-Kemp, L. (2009) 'Information security management: an entangled research challenge', *Information Security Technical Report*, Vol. 14, No. 4, pp.181–185 [online] https://doi.org/10.1016/j.istr.2010.04.005.

Culnan, M.J. and Williams, C.C. (2009) 'How ethics can enhance organizational privacy: lessons from the Choicepoint and TJX data breaches', *MIS Quarterly*, Vol. 33, No. 4, pp.673–687.

Dhillon, G. and Backhouse, J. (2000) 'Technical opinion: information system security management in the new millennium', *Commun. ACM*, Vol. 43, No. 7, pp.125–128, https://doi.org/10.1145/341852.341877.

Dhillon, G. and Torkzadeh, G. (2006) 'Value-focused assessment of information system security in organizations', *Information Systems Journal*, Vol. 16, No. 3, pp.293–314, https://doi.org/10.1111/j.1365-2575.2006.00219.x.

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, https://doi.org/10.1016/j.ijinfomgt.2009.05.003.

Elo, S. and Kyngäs, H. (2008) 'The qualitative content analysis process', *Journal of Advanced Nursing*, Vol. 62, No. 1, pp.107–115, https://doi.org/10.1111/j.1365-2648.2007.04569.x.

Eloff, J.H.P., Labuschagne, L. and Badenhorst, K.P. (1993) 'A comparative framework for risk analysis methods', *Computers & Security*, Vol. 12, No. 6, pp.597–603, https://doi.org/10.1016/0167-4048(93)90056-B.

Feldman, M.S. (2000) 'Organizational routines as a source of continuous change', *Organization Science*, Vol. 11, No. 6, pp.611–629, https://doi.org/10.1287/orsc.11.6.611.12529.

Feldman, M.S. and Pentland, B.T. (2003) 'Reconceptualizing organizational routines as a source of flexibility and change', *Administrative Science Quarterly*, Vol. 48, No. 1, p.94, https://doi.org/10.2307/3556620.

Fowler, S. (2003) 'Information classification – who, why and how?', *GIAC Security Essentials Certification (GSEC)*, No. 1.

Galbreth, M.R. and Shor, M. (2010) 'The impact of malicious agents on the enterprise software industry', *MIS Quarterly*, Vol. 34, No. 3, pp.595–612.

Gerber, M. and von Solms, R. (2005) 'Management of risk in the information age', *Computers & Security*, Vol. 24, No. 1, pp.16–30, https://doi.org/10.1016/j.cose.2004.11.002.

Gibbs, G. (2007) *Analyzing Qualitative Data*, SAGE Publications, Ltd., London, England, UK, http://www.methods.sagepub.com/book/analyzing-qualitative-data.

Goldstein, J., Chernobai, A. and Benaroch, M. (2011) 'An event study analysis of the economic impact of IT operational risk and its subcategories', *Journal of the Association for Information Systems*, Vol. 12, No. 9, p.606.

Hepsø, V., Monteiro, E. and Rolland, K.H. (2009) 'Ecologies of e-Infrastructures', *J. AIS*, Vol. 10, No. 5, p.2.

Hsu, C.W. (2009) 'Frame misalignment: interpreting the implementation of information systems security certification in an organization', *European Journal of Information Systems*, Vol. 18, No. 2, pp.140–150, https://doi.org/10.1057/ejis.2009.7.

Huberman, A.M. and Miles, M.B. (Eds.) (2002) *The Qualitative Researcher's Companion*, Sage Publications, Thousand Oaks, CA.

ISO/IEC, 27000 (2014) *ISO/IEC 27000: Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary*, ISO.

ISO/IEC, 27001 (2013) *ISO/IEC 27001: Information Technology – Security Techniques – Information Security Management Systems – Requirements*, ISO.

ISO/IEC, 27002 (2013) *ISO/IEC 27002: Information Technology – Security Techniques – Code of Practice for Information Security Controls*, ISO.

ISO/IEC, 27005 (2013) *ISO/IEC 27005: Information Technology – Security Techniques – Information Security Risk Management*, ISO.

Kaarst-Brown, M.L. and Thompson, E.D. (2015) 'Cracks in the security foundation: employee judgments about information sensitivity', *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research (SIGMIS-CPR '15)*, ACM, New York, NY, pp.145–151, DOI: https://doi.org/10.1145/2751957.2751977

Kotulic, A.G. and Clark, J.G. (2004) 'Why there aren't more information security research studies', *Information & Management*, Vol. 41, No. 5, pp.597–607 [online] https://doi.org/10.1016/j.im.2003.08.001.

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, http://dx.doi.org/10.1016/j.telpol.2009.03.002.

Kumar, R.L., Park, S. and Subramaniam, C. (2008) 'Understanding the value of countermeasure portfolios in information systems security', *Journal of Management Information Systems*, Vol. 25, No. 2, pp.241–280, https://doi.org/10.2753/MIS0742-1222250210.

Kwon, J. and Johnson, M.E. (2013) 'Health-care security strategies for data protection and regulatory compliance', *Journal of Management Information Systems*, Vol. 30, No. 2, pp.41–66, https://doi.org/10.2753/MIS0742-1222300202.

Lo, C-C. and Chen, W-J. (2012) 'A hybrid information security risk assessment procedure considering interdependences between controls', *Expert Systems with Applications*, Vol. 39, No. 1, pp.247–257, https://doi.org/10.1016/j.eswa.2011.07.015.

Lowry, P.B. and Moody, G.D. (2015) 'Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies: proposing the control-reactance compliance model (CRCM)', *Information Systems Journal*, Vol. 25, No. 5, pp.433–463, https://doi.org/10.1111/isj.12043.

Lundgren, M. (forthcoming) 'Rethinking capabilities in information security risk management: a systematic literature review', forthcoming.

Niemimaa, E. and Niemimaa, M. (2017) 'Information systems security policy implementation in practice: from best practices to situated practices', *European Journal of Information Systems*, Vol. 26, No. 1, https://doi.org/10.1057/s41303-016-0025-y.

Njenga, K. and Brown, I. (2012) 'Conceptualising improvisation in information systems security', *European Journal of Information Systems*, Vol. 21, No. 6, pp.592–607, https://doi.org/10.1057/ejis.2012.3.

Oetzel, M.C. and Spiekermann, S. (2014) 'A systematic methodology for privacy impact assessments: a design science approach', *European Journal of Information Systems*, Vol. 23, No. 2, pp.126–150, https://doi.org/10.1057/ejis.2013.18.

Ozkan, S. and Karabacak, B. (2010) 'Collaborative risk method for information security management practices: a case context within Turkey', *International Journal of Information Management*, Vol. 30, No. 6, pp.567–572.

Parker, D.B. (2007) 'Comparison of risk-based and diligence-based idealized security reviews', *EDPACS*, Vol. 36, Nos. 3–4, pp.1–12, https://doi.org/10.1080/07366980701804805.

Parnas, D.L. and Clements, P.C. (1986) 'A rational design process: how and why to fake it', *IEEE Trans. Softw. Eng.*, Vol. 12, No. 2, pp.251–257.

Puhakainen, P. and Siponen, M. (2010) 'Improving employees' compliance through information systems security training: an action research study', *MIS Q.*, Vol. 34, No. 4, pp.757–778.

Reid, R.C. and Floyd, S.A. (2001) 'Extending the risk analysis model to include market-insurance', *Computers & Security*, Vol. 20, No. 4, pp.331–339, https://doi.org/10.1016/S0167-4048(01)00411-4.

Ritchie, J. and Spencer, L. (2002) 'Qualitative data analysis for applied policy research', in Huberman, A.M. and Miles, M.B. (Eds.): *The Qualitative Researcher's Companion*, pp.173–194, Sage Publications, Thousand Oaks, CA.

Sajko, M., Rabuzin, K. and Bača, M. (2006) 'How to calculate information value for effective security risk assessment', *Journal of Information and Organizational Sciences*, Vol. 30, No. 2, pp.263–278.

Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. (2016) 'Taxonomy of information security risk assessment (ISRA)', *Computers & Security*, March, Vol. 57, No. C, pp.14–30 [online] https://doi.org/10.1016/j.cose.2015.11.001.

Shedden, P., Smith, W. and Ahmad, A. (2010) 'Information security risk assessment: towards a business practice perspective', *Proceedings of the 8th Australian Information Security Management Conference*, SECAU, 30 November [online] https://doi.org/10.4225/75/57b6769334787.

Siponen, M. (2006) 'Information security standards focus on the existence of process, not its content', *Communications of the ACM*, Vol. 49, No. 8, p.97 [online] https://doi.org/10.1145/1145287.1145316.

Spears, J.L. and Barki, H. (2010) 'User participation in information systems security risk management', *MIS Q.*, Vol. 34, No. 3, pp.503–522.

Straub, D.W. and Welke, R.J. (1998) 'Coping with systems risk: security planning models for management decision making', *MIS Quarterly*, Vol. 22, No. 4, p.441, https://doi.org/10.2307/249551.

Sutton, S.G., Khazanchi, D., Hampton, C. and Arnold, V. (2008) 'Risk analysis in extended enterprise environments: identification of critical risk factors in B2B e-commerce relationships', *Journal of the Association for Information Systems*, Vol. 9, Nos. 3–4, pp.151–174.

Swedish Civil Contingencies Agency (2014) *En Bild Av Myndigheternas Informationssäkerhetsarbete 2014 – Tillämpning Av MSB:S Föreskrifter* [*A Picture of Governmental Agencies Work with Information Security 2014 - Application of the Swedish Civil Contingencies Agency Guidelines*], Report No. 978-91-7383-478– 0, Report, Swedish Civil Contingencies Agency [online] https://www.msb.se/Produkter–tjanster/Publikationer/Publikationer-fran-MSB/En-bild-av-myndigheternas-informationssakerhetsarbete-2014/.

Tatar, Ü. and Karabacak, B. (2012) 'An hierarchical asset valuation method for information security risk analysis', in *International Conference on Information Society (i-Society 2012)*, June, pp.286–291.

Taylor, R.G. (2006) 'Management perception of unintentional information security risks', in *ICIS 2006 Proceedings – Twenty Seventh International Conference on Information Systems*, pp.1581–1598 [online] http://www.scopus.com/inward/record.url?eid=2-s2.0-84870033474&partnerID=40&md5=bb9de0ec3bc737678d023dd84116accb.

Taylor, R.G. (2015) 'Potential problems with information security risk assessments', *Information Security Journal: A Global Perspective*, Vol. 24, Nos. 4–6, pp.177–184, https://doi.org/10.1080/19393555.2015.1092620.

Taylor, R.G. and Brice, J. (2012) 'Fact or fiction? A study of managerial perceptions applied to an analysis of organizational security risk', *Journal of Organizational Culture, Communications and Conflict*, Vol. 16, No. 1, pp.1–23.

Tsohou, A., Karyda, M., Kokolakis, S. and Kiountouzis, E. (2015) 'Managing the introduction of information security awareness programmes in organisations', *European Journal of Information Systems*, Vol. 24, No. 1, pp.38–58, https://doi.org/10.1057/ejis.2013.27.

Visintine, V. (2003) *An Introduction to Information Risk Assessment*, SANS Institute, Vol. 8, p.116.

Webb, J., Ahmad, A., Maynard, S.B. and Shanks, G. (2014) 'A situation awareness model for information security risk management', *Computers & Security*, July, Vol. 44, pp.1–15, https://doi.org/10.1016/j.cose.2014.04.005.

Whitman, M.E. and Mattord, H.J. (2014) *Management of Information Security*, 4th ed., Cengage Learning, Stamford, CT, USA.

Paper C

Revisiting information security risk management challenges: a practice perspective

Bergström, E., **Lundgren, M.**, and Ericson, Å. (2019) 'Revisiting information security risk management challenges: a practice perspective,' *Information & Computer Security*, Vol. 27, Issue: 3, pp.358–372.

Revisiting information security risk management challenges: a practice perspective

Erik Bergström
School of Informatics, University of Skövde, Skövde, Sweden, and
Martin Lundgren and Åsa Ericson
Department of Computer Science, Information Systems, Luleå University of Technology, Luleå, Sweden

Received 5 September 2018
Revised 9 November 2018
21 December 2018
Accepted 8 January 2019

Abstract

Purpose – The study aims to revisit six previously defined challenges in information security risk management to provide insights into new challenges based on current practices.

Design/methodology/approach – The study is based on an empirical study consisting of in-depth interviews with representatives from public sector organisations. The data were analysed by applying a practice-based view, i.e. the lens of knowing (or knowings). The results were validated by an expert panel.

Findings – Managerial and organisational concerns that go beyond a technical perspective have been found, which affect the ongoing social build-up of knowledge in everyday information security work.

Research limitations/implications – The study has delimitation as it consists of data from four public sector organisations, i.e. statistical analyses have not been in focus, while implying a better understanding of what and why certain actions are practised in their security work.

Practical implications – The new challenges that have been identified offer a refined set of actionable advice to practitioners, which, for example, can support cost-efficient decisions and avoid unnecessary security trade-offs.

Originality/value – Information security is increasingly relevant for organisations, yet little is still known about how related risks are handled in practice. Recent studies have indicated a gap between the espoused and the actual actions. Insights from actual, situated enactment of practice can advise on process adaption and suggest more fit approaches.

Keywords Asset valuation, Information security, Practice theory, Risk management

Paper type Research paper

Introduction

Information Security Risk Management (ISRM) has been defined as a continuous process to identify and mitigate risks towards an organisation's critical information assets. More than a decade ago, Kotulic and Clark (2004) highlighted the importance of empirical studies in ISRM. Since then, little is still known about how organisations protect themselves in practice (Baskerville *et al.*, 2018). The lack of empirical understanding makes it difficult to draw insights on how organisations actually conduct ISRM, what challenges they are confronted with in their tasks, and the nature of knowledge required to mitigate them. Lately, researchers have further pointed out a need for practice-based research within the information security domain. Niemimaa (2016) and Alaskar *et al.* (2015), for example, noted that most empirical research focuses on intention rather than actual behaviour. As a result, they recommend that future studies should be conducted on actual practice to illustrate

Information & Computer Security

2056-4961
DOI 10.1108/ICS-09-2018-0106

further how management processes do not always follow the espoused pattern in standards. Similarly, Shedden *et al.* (2010) stressed in their study the importance of a practice-based perspective to ISRM to explore its effectiveness within organisations. Likewise, Alshaikh *et al.* (2018) have demonstrated an applied practice-based lens to closer align security training with the organisational context, while Öbrand *et al.* (2012) grounded their study on a practice-based approach to understand better how risk management activities emerged over time. Thus, to the best of our knowledge, a few studies have shown the potential of a practice-based lens.

A consequence when disregarding practice may lead to overvaluing the formal approaches while undervaluing situated enacted activities, i.e. how practice adapts its processes to real situations (Jarzabkowski *et al.*, 2016). One example of this can be seen in the growing misconception that compliance with formal processes is equivalent with good security (Kwon and Johnson, 2013; Webb *et al.*, 2016). Not only does this leave many organisations more concerned with accommodating rather than developing and adapting security practices tailored to their unique context (Kwon and Johnson, 2013; Webb *et al.*, 2016), it has also been shown that strictly following formal practices will be "de-skilling to practitioners because creativity and reflexivity is stifled" (Njenga and Brown, 2012, p. 594). In other words, practice is what gives actual, contextual meaning and locally produced knowledge to formal approaches, and should be studied as it has proven to provide valuable insight to ISRM for practitioners and researchers alike.

This paper aims to provide insights into new challenges that are grounded in organisational management of information security processes. The study revisits six previously defined challenges from Fenz *et al.* (2014) and, by doing so, our effort is to progress further research on practice-based theory in the ISRM field by translating challenges to reflective actions, called knowings.

This paper is organised as follows; the next section discusses current ISRM processes and associated challenges, while the section after that presents the study approach. The following section presents and discusses the empirical findings. The next section accounts for the results, i.e. proposes a number of relevant insights for practice, and the final section concludes the study.

Challenges in the current Information Security Risk Management processes

Information security risk management processes

Over the past decades, the development of various ISRM processes has gained attention in the literature (ISO/IEC 27005, 2013; Bowen *et al.*, 2006; NIST SP 800-30 2012). To be applicable in different contexts, such processes are designed to be universal in scope, focusing on "formal, rule-based descriptions of procedures to be followed" (Njenga and Brown, 2012, p. 594). Therefore, risks towards information assets are seen as something that can be controlled if managed rationally and sequentially (Coles-Kemp, 2009; Dhillon and Backhouse, 2001).

Typically, these procedures' descriptions emphasise processes for measuring and identifying valuable assets within the organisation and selecting means of controlling risks towards those assets based on predictions and historical comparisons (Baskerville *et al.*, 2014). Standards such as ISO/IEC 27005 (2013) and NIST SP 800–30 (2012) outline a continuous process to identify assets and existing countermeasures, assess risks and their likelihood to mitigate or accept those risks (ISO/IEC 27005, 2013; NIST SP 800-30, 2012). Furthermore, researchers such as Straub and Welke (1998) and Spears and Barki (2010), have similarly outlined ISRM as containing activities for identifying and prioritising information assets and security risks to implement and monitor countermeasures.

Evaluation of additional ISRM processes has also shown that there are only minor differences in their description (Fenz *et al.*, 2014). While varying in specific steps or depth, the process descriptions typically include activities for identifying and valuing assets, predicting risks and implementing adequate countermeasures (ISO/IEC 27005, 2013; Shedden *et al.*, 2010; Whitman and Mattord, 2014; Visintine, 2003; Baskerville *et al.*, 2014).

Six challenges in Information Security Risk Management

Fenz *et al.* (2014, pp. 419-422) find it achievable to theorise on the main challenges for organisations. Therefore, they propose, six current and fundamental challenges that still effect how risk managers come up with sound results. Starting from these six challenges as a frame of reference, additional input from the literature has here been used to refine each challenge's description. The refined challenges can thus be presented as follows:

Asset and countermeasure inventory. The challenge relates to the problems of identifying what would be a valuable asset to protect and what potential countermeasures could be used to protect the asset. The challenge relates to, e.g. how to identify information capital (Bunker, 2012; Ku *et al.*, 2009), especially considering that information is everywhere and can take any shape (Saxby, 2008). Additionally, most ISRM processes lack a reliable asset inventory approach (Vose, 2008) adding complexity to the challenge.

Assigning asset values. The challenge relates to the actual assignment of a value to an asset. This includes, e.g. the basics of such estimations (Aksentijevic *et al.*, 2011; Al-Fedaghi, 2008), a lack of motivation for valuation among colleagues (Hayes, 2008) and the subjective judgment (Glynn, 2011; Kaarst-Brown and Thompson, 2015) associated with it. Furthermore, the development of classifications (Baškarada, 2009) is based on too generic standards (Bayuk, 2010), which can be troublesome for organisations. Also, deciding the granularity of the information (Blyth and Kovacich, 2006) and getting it performed consistently in the organisation (Eloff *et al.*, 1996) is difficult, especially considering that technology cannot solve the problem (Everett, 2011).

Failed predictions of risk. The challenge is described in relation to an attacker's interest in the organisation's assets. That interest is hard to predict as it changes over time. Prevention of predicted threats is inherent in the actual paradigm of ISRM (Baskerville *et al.*, 2014). However, not all risks are predictable, measurable and persistent (Taylor, 2015); some are more unpredictable and better suited to interpretive approaches (Spagnoletti and Resca, 2008).

The overconfidence effect. This challenge relates to managerial issues not typically addressed in standards and frameworks (Fenz *et al.*, 2014). Challenges include managerial styles that are often grounded in being far too optimistic (Taylor, 2015; Rhee *et al.*, 2012), the authority of information security leaders (Collette, 2006; Taylor, 2015) and a lack of standards for particular sectors (Janczewski and Xinli Shi, 2002).

Knowledge sharing. This challenge relates to the necessity of sharing information in and between organisations. Awareness of this challenge can be useful in risk prediction to assess better how information and knowledge assets are put at risk (Padyab *et al.*, 2014). Knowledge sharing is important to sustain the operational complexity in risk prediction and rests both individually and collectively within people (Shedden *et al.*, 2011).

Risk vs cost trade-offs. This challenge relates to being cost-effective in balancing costs of countermeasures and the expected loss of an asset. The challenge identifies the lack of cost estimation techniques related to risk management activities as one of the main weaknesses of current risk management processes (Sadok and Spagnoletti, 2011; Lawrence *et al.*, 2003).

Study approach

Data collection

To capture reasoning in practice, a qualitative research approach was designed. To gain an understanding of organisations ISRM processes, rich insights could be based on sampling from a few respondents possessing expertise in the chosen area (Kvale, 1996; Patton, 2014). Therefore, statistical generalisations were not sought after, but instead, saturation of the chosen topics, i.e. patterns in the answers can be identified and themes reoccur (Mason, 2002).

Considering the difficulty to obtain field data on how ISRM processes are enacted in practice (Baskerville *et al.*, 2018; Kotulic and Clark, 2004), Swedish public sector organisations were chosen. The reasoning behind this was twofold. Firstly, owing to the principle of public access to official records, internal policies are generally more accessible. Secondly, the Swedish public sector is required to work systematically with ISRM; however, there is no nationally enforced standard. Thus, the public sector has adopted different ISRM approaches in practice.

The organisations included in this study were selected on the basis of their expertise and that they had well-documented policies and implemented procedures. A study on Swedish ISRM practices revealed, however, that despite being a requirement, only 60 per cent of Swedish Government agencies have an established activity for risk management, and only 43 per cent have one for asset valuation (Swedish Civil Contingencies Agency, 2014). Drawing on the result of a large survey in governmental Sweden (Bergström *et al.*, 2018), four public sector organisations were chosen for this study. Each organisation represented a different sector providing functions critical to society, and demonstrated particularly mature ISRM processes. The organisations provided their internal policy documents for analysis, which added secondary data to the study. The key responsible ISRM roles within the respective organisation were identified in parallel with the review of the internal policies and were interviewed. In three of the four organisations, the selected interviewees were also the writers of their respective internal policy. An overview of the organisations and interviewees is presented in Table I.

An interview guide was developed based on the six refined challenges. Thirty open-ended questions (Bryman and Bell, 2011) were formulated as a basis for the interviews, targeting ISRM activities and practices. The questions were open-ended to avoid imposing our perceptions on their answers. Altogether, the interviews and the internal policies gave rich insights into motivations and reasoning among the respondents.

Each interview lasted between 50 and 90 min and was recorded. The recordings were divided among the authors for transcription in its entirety and double-checked by each other, resulting in 52 pages of transcriptions.

Data analysis

The practice lens of organisational creation of meaning, in short, "knowing" or "knowings", was applied for finding the unit of analysis. Knowing is described by Orlikowski (2002, p. 249) as follows:

Table I. Background details on the organisations and interviewees

ID	Sector	No. of employees	Role(s)
Alpha	Health and social affairs	~1, 200	Security Specialist
Beta	Environment and energy	~650	Security Architect
Gamma	Enterprise and innovation	~2, 000	Information Security Coordinator, and IT-Architect
Delta	Public sector coordination	~230	Director of Preparedness and Response

> Purposive and reflexive, continually and routinely monitoring the ongoing flow of action–their own and that of others—and the social and physical contexts in which their activities are constituted.

The important perspective here is to apply knowing as a verb indicating action, doing and practice. Thus, the transcribed answers were first categorised, using concept-driven coding (Spencer and Ritchie, 2002). The categorised material was then discussed and merged into a new document and thematised into themes of knowing through the practice-based lens, emphasising enacted activities that got "their work done".

Validation

In ISRM research, there is a general lack of validation, and there are various approaches on how to perform it (Fenz and Ekelhart, 2011). Silverman (2015) recommends qualitative research approaches to take the results "back to the people" to see if they conform to their own experiences. Similarly, Fenz and Ekelhart (2011) suggest that expert panels are a good approach for validating ISRM results as it is one of the few ways that accounts for various real-world parameters.

Hence, to validate the knowings and practices that met the refined challenges in practice, opinions were sought from a broader set of information security managers. An expert panel consisting of 16 senior information security managers from public sector organisations was organised. None of the participants in the expert panel came from the four organisations targeted in this study. The expert panel consisted of nine chief information security officers, two chief technology officers, and the remaining five had other various information security management roles.

The expert panel was held as an hour-long session, where the authors presented how the challenges had been met in practice, followed by discussions. The session was recorded and transcribed.

Empirical results

One of the common pitfalls in practice-based research is taking the existence of isolated entities for granted (Feldman and Orlikowski, 2011). To address this, the empirical result was divided into its respective challenge and referenced to the organisation making a claim.

Asset and countermeasure inventory

The investigated organisations acknowledge the difficulty in identifying information assets with high granularity. They have instead moved towards identifying the systems in which the information resides in, to abstract the level of detail and by having a direct relation between asset values and countermeasures. This approach rests on the belief that different information types may exist within the same system, and that it makes sense for them to value the whole system based on the most sensitive information present in the system. A consequence is that they over-protect some information, but the difficulty of implementing a variety of countermeasures matching the different valuations on the same system is a greater challenge and considered a less effective use of resources.

Alpha and Beta both emphasised that they perform an in-depth initial identification of all infrastructure systems present in their respective organisations, and are valuing the infrastructure with regard to present or needed countermeasures. They explained that this approach makes the system identification, and hence the subsequent valuation easier. Because all information flows and connections in entangled systems do not need to be

investigated as thoroughly, since the information flows will inherently be protected if the infrastructure is protected. Alpha justified this as follows:

> Instead of digging down in each individual [information] flow, every row, [. . .] I mean if you do not have matching countermeasure levels later [. . .] [which is] a common approach to valuation, what's the meaning by noticing the difference [in value] between different rows?

Another motivation for the system identification approach was given by Gamma who believed that it can be seen as positive when some information is over-valued and henceforth over-protected in a system as it is considered too hard to capture all changes to the asset value over time in its life-cycle.

An additional insight also came from Gamma that pointed out that the organisation does not necessarily have to invest in identifying and valuing all information, but rather do it on-demand and to start where it gives the most "bang for the buck". For example, if there are changing risks to a system, it could, as clarified by Gamma, trigger a new valuation.

The investigated organisations can be said to have a viewpoint where the valuation of the identified information is not separated from countermeasures, but rather that countermeasures are a consequence of the valuation. The organisations have either established a direct link in their internal policies between information value and specific countermeasures, or they have a clear understanding of what certain information values would require regarding countermeasures. Beta, for example, expressed this as follows: "and then, from the valuations, we knew what kind of information [we possessed], and then we also knew what types of protection we wanted to apply". Furthermore, both Beta and Delta highlighted that it is important also to perform an inventory of laws and regulations that affect the organisation as they can be used as a motivation for defining minimum requirements on countermeasures.

It was also pointed out by the investigated organisations that one should be aware that the implemented countermeasures reflect a snapshot in time of the system and that countermeasures effectivity and information values change over time. Beta pointed out that either they have to do new valuations regularly over time or it has to be incident-driven so that systems that are often affected by incidents have to be revalued.

Assigning asset values

The organisations have all spent considerable effort in establishing the groups performing the valuation, finding ways to motivate the employees, and defining the role of the valuation in the ISRM process.

Determining the value of information assets is described in the literature as difficult and problematic because of the subjective judgment that has to be made. The investigated organisations suggested that a concrete way of reducing this subjectivity is to have a clearer link between information types and countermeasures as described earlier, in which specific countermeasures match the consequence of a valuation. The benefit of using predefined values for certain information types, which also increase consistency, throughout the organisation, align with the suggested approach.

Similar to the findings in the challenge of inventory of assets and countermeasures, the organisations that chose a system valuation approach allows a larger group with diverse skills and experiences to participate and highlight the information in a system, and its use from several perspectives. Such a group-based workshop approach with open discussions has been adopted by the investigated organisations. Gamma adds that the workshops are trying to consider the information life-cycle to capture all stakeholders. The group-based workshops invite, for example, lawyers in the valuation process at both Beta and Gamma.

Beta invites many different competencies, or in their terms, "the right people" to the valuations, to get an as unbiased view as possible of the information assets in question, including those finally responsible for implementing the countermeasures. Ultimately, whom to involve in the workshop depends on what system is being valued and which stakeholders it addresses. Gamma also states that it is important to understand that group composition is something that will take shape over time and that one cannot specify the participants from the very beginning.

The respondents expressed that it is difficult to motivate employees to perform the valuation. Alpha has tackled this challenge by following up the results of the valuation and by making the results visible throughout the entire ISRM process. In Alphas words, the valuation

> Is important, and considering the time it takes, it should result in something more than just putting a label on the information. Otherwise, everyone will start wondering; 'Ok, this information was so important, what happens now? Why don't they care about it half a year later?' So it is very important that it is actually followed-up [. . .] so that the organisation can confirm throughout the [ISRM] process.

An important additional aspect is to ensure that there is a clear output of the valuation that goes into the risk prediction, not only the numeric value itself but also contextual information about usage and users to help motivate countermeasures.

Failed predictions of risk

Contrary to suggestions from the literature on ISRM processes, none of the organisations conducted risk prediction in the suggested way. Risk prediction was seen as a complex and highly time-consuming activity. Because of this, it became mostly an activity to rank pre-determined countermeasures to be implemented on the basis of a fixed list of risks, and not applied as an activity to uniquely choose countermeasures based on risk predictions.

However, both Alpha and Beta used to conduct risk prediction but soon found that the same or similar risks appeared each time. Consequently, Beta stopped conducting risk predictions on smaller systems unless there was a reason to believe that a particular system was targeted by unexpected risks. Instead, Beta abstracted their component for analysis to entire infrastructures. Beta argued that "we have a pretty good understanding of what assets are important within the infrastructure, so it makes sense to focus the risk prediction on the infrastructure". Furthermore, Alpha does not use risk prediction to decide on final countermeasures. Instead, they have correlated particular asset values with particular countermeasures. Nevertheless, risk prediction still plays a part in Alpha's work, but merely as a filter to determine in what order to implement the countermeasures. Previously, Alpha used to have an algorithm to help calculate and prioritise what countermeasures to implement. However, as no one in the organisation used it, the responsibility of determining the order of countermeasures to implement came to rest with the system owner. Interestingly, Beta and Alpha recognise that their current approach might not provide as much detail as otherwise characterised by traditional approaches in risk prediction. Alpha states that they will inevitably "miss maybe 5 per cent of risks that are never found, and the only way to find them is to make unique risk predictions", yet they conclude, "[. . .] our way of doing it still covers most of all risks, and it provides much better use of resources".

Delta and Alpha argue that software tools could only theoretically help to conduct risk prediction, but would be practically infeasible. They build their argument on the notion that a continuous stream of risk predictions is not reasonable considering the required implementation and monitoring of countermeasures. Alpha describes that

> Even though I could wish that we had risk prediction software [. . .] no, that is not for us. When we work with this in practice, after an asset has been valued, several countermeasures are already mandated, something that can take 6-18 months to implement.

Beta notes that the skills for how to manage risk are not easily shared, something they have spent much time trying to perfect. The only successful approach, according to Beta, is to simply exercise risk management over a long period to reach organisational fit.

The overconfidence effect

To overcome some of the challenges posed by the overconfidence effect, the organisations had, to avoid ambiguity, developed a clear ISRM process accompanied by tailored guidelines and expectations for daily work. Additionally, top managers were assigned responsibilities for final decisions on organisation-wide countermeasures.

Alpha, for example, use established formats describing the relations between asset values and specific countermeasures. This documentation has, in turn, removed some of the ambiguous decision-making in finding suitable countermeasures. Consequently, top managers decide the final risk acceptance, and will also be responsible for determining additional countermeasures that go outside what has been established. This has made the process more transparent to the entire organisation. Similarly, for Gamma, this has also worked as a motivator in sanctioning additional economic support from top managers.

In an effort to cultivate the established ISRM process, Alpha and Beta have, as they describe, dedicated plenty of resources trying to educate employees about its activities through workshops and tailored guidelines. Alpha expresses that having a clear, detailed outlined ISRM process is key to success as "it gives a clear benefit for the organisation, and the organisation itself experience the [ISRM] process as something that adds value and is of use for them". Alpha even indicates that they do not want an extensive "ISRM manual" but rather target-oriented instructions for all employees. Gamma takes it one step further and uses an approach that can be described as need-to-know, where only the closest ones will learn about, for example, how to perform the valuation. Beta similarly develops their guidelines by tailoring it to the targeted employees by elaborating questions such as "How would these requirements be met and understood by the targeted audience?" and "How can we change it to make the message clearer?".

An organisation-wide understanding of the ISRM activities affected Alphas and Betas' attitude towards information security. Rather than seeing ISRM as a hindrance or something only necessary to abide by laws and regulations, ISRM was believed to have ethical or moral consequences. In Betas case, for example, compliance was motivated because there could be dangerous consequences in the real world if systems were not adequately protected. Similarly, Alpha had a culture of *quis custodiet ipsos custodes* (who will guard the guardian). For example, during system development, intended system owners will critically review the predefined requirements in a series of dialogues with the developers. Because the system will ultimately be assessed by a champion to assure its countermeasures, developers and future owners have realised that any shortcuts will inevitably be more costly in the end for both parties.

Knowledge sharing

An important aspect of tackling the challenge of knowledge sharing is how to accomplish a coherent ISRM process in practice. All the organisations stressed the importance of including a champion with key skills in all the activities of the ISRM process, making these champions the glue that makes the processes coherent. The investigated organisations saw different champions. For example, Alpha saw a security specialist as a champion, while

Gamma saw an IT architect. Having a champion contribute to reducing problems with different views on asset valuations, and offer an inherent possibility of monitoring the whole ISRM process. Beyond a champion, it was also stressed that the organisational side with its knowledge of how and by whom certain information is used, together with the IT department with its technical know-how, are represented and participate throughout the whole ISRM process. This knowledge does not need to be in-house, as shown by both Delta and Gamma. Instead, they collaborate closely with other similar organisations within their respective sectors, to borrow and share competence when needed, such as technical know-how for a particular system.

Beta expressed that they have dialogues that are not part of the formal ISRM process, but that add insight. For example, when systems are being procured or developed, an effort to capture requirements, or perform preliminary valuations are made. These informal dialogues are initiated either by the champions, from the procurement or development side. It is viewed by Beta as a sign of a mature ISRM process because the champions do not have knowledge of everything in progress within the organisation and point out that it also limits the risk of having the ISRM process rely solely on a particular champion.

Another knowledge-sharing enabler described was that the organisations chose to homogenise their language internally, i.e. a shared vocabulary, to avoid misunderstandings. An example of this is how information types and risk activities were referred to by the respective organisations, both in the interviews and in their written policies. Delta described it as follows:

> We have some kind of definition [of key concepts] that we cannot get crystal clear, there are always grey areas, but as far as we can, we try to define what we mean by different concepts.

Risk vs cost trade-offs

The investigated organisations see countermeasures as a result of the valuation. Therefore, the discussion about cost does not derive from risk but rather the asset valuation. Because of this, the discussion focused on the cost associated with countermeasures, and not risks.

Although the relation between asset value and countermeasures were perceived as obvious, the cost trade-off in practice was not. This was shown through various examples, as for instance at Gamma, they perceived their policy as running short with respect to cost consequence, or as they described it:

> The policy for assigning asset values are clear and easy to follow, [. . .] but I think there is still something missing, some parameter for reaching a decision on countermeasures in terms of time and money.

Gamma further described that it is common that this ambiguity, in the end, leads to more time spent on searching for less expensive countermeasures. Beta explained that instead of looking for less expensive countermeasure alternatives, they reconsider the asset value altogether when facing the challenge of cost trade-off. Alpha clarified that they already deal with this challenge during the valuation by including an economic perspective by calculating the estimated economic consequences of a loss. The resulting estimated cost helps justify expensive countermeasures for top managers.

Alpha, Beta and Delta express that this challenge can be met by establishing national requirements, by relating certain information types with particular countermeasures. Such requirements would decrease the uncertainty, as explained by Beta, "by stating that 'these countermeasures are standardised in Sweden,' because then you can say 'this information

shall be protected using these countermeasures,' so that everybody knows what is expected".

Finally, the organisations highlighted the cost of the ISRM process itself. To achieve a coherent process that matures over time, both time and money have to be allocated.

Insights for practice

By analysing the empirical result, a set of knowings can be formulated that describe the enacted practice of how the challenges are reflected upon and how the ongoing collective flow of actions and reasoning create a rationale for the work. The connection between challenges, how they are met in practice and how knowings are constituted are outlined in Table II below.

These identified challenges and suggested knowings have theoretical and practical implications, as follows:

Knowing how to be "good enough": because security is not following a recipe of fortification, but are efforts to apply its principles in the organisations daily work. The organisations described countermeasures as "a snapshot" whilst also acknowledging that they change over time. Recognising that there was no recipe to follow, reaching a "good enough" mentality would, therefore, ensure security processes to be refined and adapted. Not recognising this could be a reason why organisations often perceive security as an obstacle rather than a support. For example, valuing systems instead of information results in less time spent on identification and more time spent on assigning asset values. According to the expert panel in the validation, this approach also resonates better with services where control over the security controls are outsourced. For example, cloud services were mentioned as such services where the security controls many times are pre-determined by the service provider. Directly associating valuation with countermeasures becomes a natural effect of using such services. Furthermore, directly associating valuation with countermeasures removes some of the ambiguity in the asset valuation. Therefore, systems or entire infrastructures were mainly targeted for identification. Finally, the practice of making an initial in-depth identification of infrastructure was recognised in the discussion, but it was pointed out that it could lead to overprotecting parts of the infrastructure, which, in turn, cost more money for the organisation.

Knowing how to hurry slowly: because ISRM implementation costs time and money. It takes time to find which stakeholders to include and to what extent, what competence is required and the time it takes to put together a team. This can be seen as overwhelming if the work does not progress at a pace that is aligned with the rest of the organisation. One such example was described by an expert during the validation, where their organisation had suffered from an information overflow when attempting to valuing all information at the beginning of their ISRM process. Whilst it is tempting to assume managers will make correct and rational decisions at the early beginning of the ISRM process, such overconfidence could pressure managers to make hasty decisions that could be more costly in the long run. Similarly, investing in countermeasures can give an instant result, but lower security over time if compared with investing in an organisationally fit ISRM implementation. Instead, the experts agreed that it might be better to start out slowly with a few critical systems and learn from this process before proceeding with other systems in the organisation. Identify and assign champions could, however, help balance the implementation by both double check the ISRM progress and the overall organisational fit of the ISRM process.

Knowing there is no silver bullet: because it is often suggested to use software tools to help assess risks, countermeasures and assets, the interviewees said that such tools seldom take

Challenges from Fenz *et al.* (2014)	Challenges as met in practice	Knowings constituted in the practice
Asset and countermeasure inventory	Raise the abstraction level by identifying the most sensitive information types in systems	Knowing how to be "good enough"
	An initial in-depth identification of all infrastructure makes valuation easier	Knowing how to be "good enough"
	Make valuation on-demand where it gives most "bang for the buck"	Knowing there is no silver bullet
	Be aware that implemented countermeasures reflect a snapshot in time	Knowing how to be "good enough"
Assigning asset values	Use predefined valuations for certain information types to create a direct relation between valuation and countermeasures	Knowing how to be "good enough"
	Accepting that a coherent ISRM implementation cost time and money	Knowing how to hurry slowly
	Use workshops with diverse skills and experiences when valuing	Knowing how to hurry slowly
	Follow up the valuation throughout the ISRM process to support and motivate employees	Knowing the bigger picture
Failed predictions of risk	Risk prediction reduced to rank pre-determined countermeasures based on a fixed list of risks	Knowing how to be "good enough"
	Being completely updated on real-world risks is practically infeasible	Knowing there is no silver bullet
	Favour simplicity over complexity and accept not all risks can be found	Knowing how to be "good enough"
The overconfidence effect	Clear ISRM process with tailored guidelines and training	Knowing the bigger picture
	Top managers make final decisions of countermeasures	Knowing the bigger picture
	Top managers own risk acceptances	Knowing the bigger picture
	Ethical and moral consequences motivate the ISRM process more than laws and regulations	Knowing there is no silver bullet
Knowledge sharing	Identify a champion with key ISRM skills	Knowing how to hurry slowly
	Champions are the glue that makes the ISRM process coherent	Knowing the bigger picture
	Informal dialogues are encouraged to reach common expectations about the ISRM activities	Knowing the bigger picture
	Homogenise the internal language to avoid misunderstandings	Knowing the bigger picture
Risk vs cost trade-offs	Cost associated more with countermeasures than risks as the trade-off is made between countermeasures and the economic consequences of information loss	Knowing how to be "good enough"

Table II.
An overview of the empirical results highlighting ISRM challenges as found in literature, how they are met in practice, and constituted as knowings

social or organisational aspects into account. For example, this was shown where organisations had moved beyond using or even wanting to use, such tools because it was not feasible in daily work, e.g. it did not give a return on investment, i.e. "bang for the buck". Staying updated about, e.g. all real-world risks were not found to be the main issue, but rather the time required to act upon them. Similarly, being completely updated on real-world risks does little to socially motivate actions. Instead, risk is too subjective to be beneficial by

simply being updated, and requires practical experience, or knowings, which can only be obtained over time. It was, for example, shown that requirements such as laws and regulations, did not motivate the ISRM process, but intrinsic values did. The expert panel confirmed this and acknowledged the importance of emphasising ethical and moral consequences. However, they had a lengthy discussion on the difficulty in recognising such intrinsic values for different groups. For instance, when motivating economists, economic consequences could be more beneficial to use than ethical and moral consequences.

Knowing the bigger picture: because the various activities within ISRM should be enacted as a holistic entity that is aligned with the organisation's goal. Recognising that the ISRM process is more than the sum of its activities was seen as mature praxis. One should not see each activity within the process as producers and consumers of input and output but as decisions that are shaped and reshaped. In other words, it means realising that organisational alignment is the result of joint effort throughout the entire process, with active feedback from champions, informal dialogues, workshops and training activities to reach unanimous ideas and expectations. Several members of the expert panel were champions in their respective organisations and gave additional input on how to achieve this in practice. For example, at the start of a valuation or risk prediction, they gave an introduction regarding the aim, objective and expectations of the task at hand to raise the participants' level of understanding. Activities such as these are seen as a dynamic learning process that is kept alive. Thereby, the activities make sense for the organisation. One example of this is that it is difficult to know exactly whom to include, something that will become clearer over time as the ISRM process evolves, which was also acknowledged by the expert panel.

Conclusions

This paper aimed to provide insights into new challenges that are grounded in organisational management of information security processes. The study revisited six previously defined challenges (Fenz *et al.*, 2014) and, by doing so, the effort was to progress further research on practice-based theory by translating challenges to reflective actions, called knowings. These have been formulated as knowing to be "good enough", knowing to "hurry slowly", knowing "there is no silver bullet" and knowing the "bigger picture". In this paper, it was thus illustrated how a practice-based lens could contribute to further insights into how context could shape practice. That is to say, content within management processes is not created by the espoused descriptions found in standard approaches but in practice formed by employees' ambition, intent and experiences. This was observed empirically, and validated by an expert panel, in which the relationship between activities as well as their content evolved as a result of what "made sense" for the practitioners. Hence, one implication for research is that much can be learned by focusing on what people do in practice, as opposed to what they should do. The identified knowings offer a base for further research in this respect.

Studies on practice, as shown here, may have the potential to be realised by practitioners and managers who are struggling with ISRM implementation (Shedden *et al.*, 2010). This paper has described examples of how a practice-based lens can provide actionable advice. It is stressed in formal standards that ISRM processes should align with organisational objectives, but there is little advice on how to do that in practice. One implication for practitioners that can be seen here is that the examples emphasise that everyone involved in the actions contribute to a shared understanding that benefits organisations. The investigated organisations showed various reflective actions to overcome such challenges, for instance, by using informal dialogues to reach common expectations about the ISRM activities or by homogenising the internal language to avoid misunderstandings, as shown in knowing "the bigger picture". Another implication for practice is that allocating resources

to identify whom to include in the process would probably benefit the subsequent work and provide for a less biased result. This was observed in practice by the use of champions, and workshops where it was emphasised to "hurry slowly". Finally, a third implication for practice is that "good enough" combined with continuous reflections could be a doable approach to deal with the fact that risks and thus also the countermeasures change over time.

References

Aksentijevic, S., Tijan, E. and Agatic, A. (2011), "Information security as utilization tool of enterprise information capital", *Proceedings of the 34th International Convention MIPRO*, 23-27 May, pp. 1391-1395.

Al-Fedaghi, S. (2008), "On information lifecycle management", *Proceedings from the 2008 Asia-Pacific Services Computing Conference*, 9-12, December, pp. 335-342.

Alaskar, M., Vodanovich, S. and Shen, K.N. (2015), "Evolvement of information security research on employees' behavior: a systematic review and future direction", *Proceedings of the 48th HI International Conference on System Sciences*, pp. 4241-4250.

Alshaikh, M., Maynard, S.B., Ahmad, A. and Chang, S. (2018), "An exploratory study of current information security training and awareness practices in organizations", *Proceedings of the 51st HI International Conference on System Sciences*, pp. 5085-5094.

Baškarada, S. (2009), "Analysis of data", Information Quality Management Capability Maturity Model, Vieweg+Teubner, pp. 139-221.

Baskerville, R., Rowe, F. and Wolff, F.-C. (2018), "Integration of information systems and cybersecurity countermeasures: an exposure to risk perspective", *ACM Sigmis Database: The Database for Advances in Information Systems*, Vol. 49 No. 1, pp. 33-52.

Baskerville, R., Spagnoletti, P. and Kim, J. (2014), "Incident-centered information security: managing a strategic balance between prevention and response", *Information and Management*, Vol. 51 No. 1, pp. 138-151.

Bayuk, J. (2010), "The utility of security standards", paper presented at 2010 IEEE International Carnahan Conference on Security Technology (ICCST), 5-8 October.

Bergström, E., Anteryd, F. and Åhlfeldt, R.-M. (2018), "Information classification policies: an exploratory investigation", in Dhillon, G. and Samonas, S. (Eds), *Proceedings of the Annual Information Institute Conference, Las Vegas, NV*, 26-28 March 2018, pp. 26-28.

Blyth, A. and Kovacich, G.L. (2006), "IA and software", *Information Assurance*, Springer London, pp. 191-212.

Bowen, P., Hash, J. and Wilson, M. (2006), *Information Security Handbook: A Guide for Managers*, National Institute of Standards and Technology, Gaithersburg, MD.

Bryman, A. and Bell, E. (2011), *Business Research Methods*, 3rd ed., Oxford University Press, USA.

Bunker, G. (2012), "Technology is not enough: taking a holistic view for information assurance", *Information Security Technical Report*, Vol. 17 Nos 1/2, pp. 19-25.

Coles-Kemp, L. (2009), "Information security management: an entangled research challenge", *Information Security Technical Report*, Vol. 14 No. 4, pp. 181-185.

Collette, R. (2006), "Overcoming obstacles to data classification [information security]", *Computer Economics Report (International Edition)*, Vol. 28 No. 4, pp. 8-11.

Dhillon, G. and Backhouse, J. (2001), "Current directions in IS security research: towards socio-organizational perspectives", *Information Systems Journal*, Vol. 11 No. 2, pp. 127-153.

Eloff, J.H.P., Holbein, L.R. and Teufel, S. (1996), "Security classification for documents", *Computers and Security*, Vol. 15 No. 1, pp. 55-71.

Everett, C. (2011), "Building solid foundations: the case for data classification", *Computer Fraud and Security*, Vol. 2011 No. 6, pp. 5-8.

Feldman, M.S. and Orlikowski, W.J. (2011), "Theorizing practice and practicing theory", *Organization Science*, Vol. 22 No. 5, pp. 1240-1253.

Fenz, S. and Ekelhart, A. (2011), "Verification, validation, and evaluation in information security risk management", *IEEE Security and Privacy Magazine*, Vol. 9 No. 2, pp. 58-65.

Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. (2014), "Current challenges in information security risk management", *Information Management and Computer Security*, Vol. 22 No. 5, pp. 410-430.

Glynn, S. (2011), "Getting to grips with data classification", *Database and Network Journal*, Vol. 41 No. 1, pp. 8-9.

Hayes, J. (2008), "Have data will travel - [IT security]", *Engineering and Technology*, Vol. 3 No. 15, pp. 60-61.

ISO/IEC 27005 (2013), "Information technology – security techniques – information security risk management", ISO/IEC.

Janczewski, L. and Xinli Shi, F. (2002), "Development of information security baselines for healthcare information systems in New Zealand", *Computers and Security*, Vol. 21 No. 2, pp. 172-192.

Jarzabkowski, P., Kaplan, S., Seidl, D. and Whittington, R. (2016), "On the risk of studying practices in isolation: linking what, who, and how in strategy research", *Strategic Organization*, Vol. 14 No. 3, pp. 248-259.

Kaarst-Brown, M.L. and Thompson, E.D. (2015), "Cracks in the security foundation: Employee judgments about information sensitivity", *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, Newport Beach, ACM, CA*, pp. 145-151.

Kotulic, A.G. and Clark, J.G. (2004), "Why there aren't more information security research studies", *Information and Management*, Vol. 41 No. 5, pp. 597-607.

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.

Kvale, S. (1996), *InterViews: An Introduction to Qualitative Research Interviewing*, SAGE Publications, Thousand Oaks, CA.

Kwon, J. and Johnson, M.E. (2013), "Health-care security strategies for data protection and regulatory compliance", *Journal of Management Information Systems*, Vol. 30 No. 2, pp. 41-66.

Lawrence, A.G., Martin, P.L. and Tashfeen, S. (2003), "A framework for using insurance for cyber-risk management", *Commun. ACM*, Vol. 46 No. 3, pp. 81-85.

Mason, J. (2002), *Qualitative Researching*, 2nd ed., SAGE Publications, London.

Niemimaa, E. (2016), "A practice lens for understanding the organizational and social challenges of information security management", *Pacific Asia Conference on Information Systems*, pp. 58-68.

NIST SP 800-30 (2012), *Guide for Conducting Risk Assessments*, National Institute of Standards and Technology, Gaithersburg, MD.

Njenga, K. and Brown, I. (2012), "Conceptualising improvisation in information systems security", *European Journal of Information Systems*, Vol. 21 No. 6, pp. 592-607.

Öbrand, L., Augustsson, N.P., Holmstrom, J. and Mathiassen, L. (2012), "The emergence of information infrastructure risk management in IT services", *Proceedings of the 45th HI International Conference on System Sciences*, 4-7 January, pp. 4904-4913.

Orlikowski, W.J. (2002), "Knowing in practice: enacting a collective capability in distributed organizing", *Organization Science*, Vol. 13 No. 3, pp. 249-273.

Padyab, A.M., Päivärinta, T. and Harnesk, D. (2014), "Genre-based assessment of information and knowledge security risks", in *Proceedings of the 47th HI International Conference on System Sciences*, 6-9 January, pp. 3442-3451.

Patton, M.Q. (2014), *Qualitative Research and Evaluation Methods: Integrating Theory and Practice*, SAGE Publications, Thousand Oaks, CA.

Rhee, H.-S., Ryu, Y.U. and Kim, C.-T. (2012), "Unrealistic optimism on information security management", *Computers and Security*, Vol. 31 No. 2, pp. 221-232.

Sadok, M. and Spagnoletti, P. (2011), "A business aware information security risk analysis method", in D'Atri, A., Ferrara, M., George, J.F. and Spagnoletti, P. (Eds), *Information Technology and Innovation Trends in Organizations*, Physica-Verlag HD, Heidelberg, pp. 453-460.

Saxby, S. (2008), "News and comment on recent developments from around the world", *Computer Law and Security Review*, Vol. 24 No. 2, pp. 95-110.

Shedden, P., Scheepers, R., Smith, W. and Ahmad, A. (2011), "Incorporating a knowledge perspective into security risk assessments", *VINE Journal of Information and Knowledge Management Systems*, Vol. 41 No. 2, pp. 152-166.

Shedden, P., Smith, W. and Ahmad, A. (2010), "Information security risk assessment: towards a business practice perspective", paper presented at Australian Information Security Management Conference 2010.

Silverman, D. (2015), *Interpreting Qualitative Data*, Sage.

Spagnoletti, P. and Resca, A. (2008), "The duality of information security management: fighting against predictable and unpredictable threats", *Journal of Information System Security*, Vol. 4 No. 3, pp. 46-62.

Spears, J.L. and Barki, H. (2010), "User participation in information systems security risk management", *Mis Quarterly*, Vol. 34 No. 3, pp. 503-522.

Spencer, L. and Ritchie, J. (2002), "Qualitative data analysis for applied policy research", in Huberman, A.M. and Miles, M.B. (Eds), *Analyzing Qualitative Data*, Routledge, Thousand Oaks, CA, pp. 187-208.

Straub, D.W. and Welke, R.J. (1998), "Coping with systems risk: security planning models for management decision making", *Mis Quarterly*, Vol. 22 No. 4, pp. 441-469.

Swedish Civil Contingencies Agency (2014), "En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter [a picture of governmental agencies work with information security 2014 – application of the Swedish civil contingencies agency guidelines]", Swedish Civil Contingencies Agency.

Taylor, R.G. (2015), "Potential problems with information security risk assessments", *Information Security Journal: A Global Perspective*, Vol. 24 Nos 4/6, pp. 177-184.

Visintine, V. (2003), "An introduction to information risk assessment", SANS institute, Vol. 8.

Vose, D. (2008), *Risk Analysis: A Quantitative Guide*, John Wiley and Sons.

Webb, J., Maynard, S.B., Ahmad, A. and Shanks, G. (2016), "Foundations for an intelligence-driven information security risk-management system", *JITTA: Journal of Information Technology Theory and Application*, Vol. 17 No. 3, p. 25.

Whitman, M.E. and Mattord, H.J. (2014), *Principles of Information Security*, 5th ed., Cengage Learning.

Corresponding author
Erik Bergström can be contacted at: erik.bergstrom@his.se

Paper D

Stress Amongst Novice Information Security Risk Management Practitioners

Bergström, E., **Lundgren, M**. (2019) 'Stress Amongst Novice Information Security Risk Management Practitioners,' *Int. Journal on Cyber Situational Awareness*, Vol. 4, No. 1, pp.128–154.

Stress Amongst Novice Information Security Risk Management Practitioners

Erik Bergström[1] and Martin Lundgren[2]

[1]Department of Computer Science and Informatics, School of Engineering, Jönköping University, Jönköping, Sweden
[2]Department of Computer Science, Luleå University of Technology, Luleå, Sweden

ABSTRACT

Today, information is a key asset for many organisations. Reducing risks of information compromise is increasingly prioritised. However, there is an incomplete understanding of how organisations with limited security knowledge and experience manage information security risks in practice. Previous studies have suggested that security-novice employees faced with burdensome, complex, and ambiguous security requirements can experience security-related stress (SRS), and ultimately influence their security decisions. In this study, we further this research stream by suggesting that SRS can similarly be found with security-novice managers responsible for developing and practising information security risk management (ISRM). Two organisations were targeted in the study using a case study approach, to obtain data about their practices, using SRS as an analytical lens. The study found various examples where SRS influenced security-novice managers' decisions, and identifies several stressors and stress inhibitors in the ISRM process and supporting ISRM tools, and discusses the implications for practitioners.

Keywords: *Security-novice, information security, information security risk management, stress, tools, compliance, management.*

Published online: 2nd December 2019

1 INTRODUCTION

Information Security Risk Management (ISRM) is relevant for organisations looking at expanding their operational capacity through digitalisation (Schirrmacher, Ondrus, & Tan, 2018). Digitalisation has impacted the way real-time information can be exchanged globally, and many organisations have embraced the innovation of new services as part of their competitive advantage and growth (Barrett, Davidson, Prabhu, & Vargo, 2015), (Gulati & Soni, 2015). Digitalisation thus holds many opportunities, but with this development, new types of risks have emerged. The effective consumption and reliable production of information that comes with digital services have become an increased target of cybercriminal activities (Schirrmacher et al., 2018). Hence, to exploit the opportunities of digitalisation, it is important first to assess what risks they hold.

ISRM is the continuous process of identifying and countering security risks to the availability, confidentiality and integrity of information (Visintine, 2003), (Whitman & Mattord, 2014). The literature often depicts ISRM as activities performed in a rational, predominantly instrumental, fashion (Lundgren & Bergström, 2019a). Considering information being among an organisation's most critical business resources (Broderick, 2001), the role and importance of ISRM as an integral part of an organisation's digital development and growth should be noted. This need for security has also been recognised by practitioners, researchers, and lawmakers, as well as end-users trusting these services (Goel & Chen, 2008), (Kim, Yim, Sugumaran, & Rao, 2016), (Lekkas, Katsikas, Spinellis, Gladychev, & Patel, 1999). As a result, ISRM has received much research attention. This has, in turn, resulted in numerous standards for how to conduct ISRM (Gikas, 2010), alongside the development of various tools to aid in its enactment (Gritzalis, Iseppi, Mylonas, & Stavrou, 2018). Such tools could be, for example, worksheets, document templates, or software designed to assist in the ISRM process and to elaborate on its activities (Gritzalis et al., 2018), (Wangen, 2017).

While there is literature on how practitioners should conduct ISRM, there is little on how they actually perform ISRM (Shedden, Smith, & Ahmad, 2010). Additionally, there is not much research on ISRM from a security-novice perspective (Osborn & Simpson, 2018). Previous studies have, however, highlighted, for some time, concerns among organisations with limited security awareness or experience when deciding about or developing their digital services (Osborn & Simpson, 2018), (Labuschagne & Eloff,

2000). Osborn and Simpson (2018), for example, found that novice practitioners were uncertain about developing or outsourcing digital services because they felt they lacked an understanding of the consequences and limitations of the developed services or agreed terms. Although security has become an important aspect for many organisations, a lack of security skills, perception or awareness can make ISRM processes complex, and difficult to understand and follow (Osborn & Simpson, 2018). Something which could cause "Security-Related Stress" (SRS) (D'Arcy, Herath, & Shoss, 2014).

SRS was originally used to explore employees' security violations caused by burdensome, complex, and ambiguous information security requirements (D'Arcy et al., 2014). In their study, D'Arcy et al. (2014) argue that employees' lack of security experience and knowledge, and the security requirements demanded of them, could result in SRS and influence their security decisions. Considering that many ISRM processes have been shown to require a great amount of expertise to apply (Wangen, 2017), (Shedden et al., 2010), and that it is often carried out by the on-site personnel and non-experts (Wangen, 2017), we propound that ISRM could similarly be experienced as burdensome, complex, and ambiguous by the practitioners involved, and thus influence their decisions too. In particular, if the practitioners are novice and lack security experience and knowledge. However, it remains unclear if and how ISRM is affected by security-novice practitioners' SRS. In this study, therefore, this research stream is furthered by exploring security-novice practitioners' enactment of ISRM, using SRS as an analytical lens. A case study was performed, in which two security-novice organisations were observed during the starting of their ISRM activities. We further discuss and propose possible causes of stress, but also potential stress inhibitors, that in some way affected ISRM activities in practice. The findings were subjected to validation, consisting of a panel with additional security-novice practitioners.

The study is outlined as follows. Section 2 introduces the background of ISRM processes and discusses tools designed to aid its practical enactment, and SRS. Section 3 presents the research approach, followed by Section 4, which presents the empirical results. This is followed by Section 5, which discusses the results, and finally, Section 6 highlights the study's conclusions and implications.

2 BACKGROUND

Most organisations are today dependent on effective production and reliable consumption of information. Decisions based on incorrect information due to wrongful manipulation, lack of information due to unavailability, or loss

of confidentiality due to information that has fallen into the wrong hands, can cause severe setbacks to an organisation (Gerber & Solms, 2001). In this section, therefore, management of such information security threats is discussed, alongside the usage of tools designed to aid in its processes, and potential dimensions of stress caused by the enactment.

2.1 Information Security Risk Management Processes

As outlined above, ISRM is the overall, continuous process to analyse and address risks to an organisation's confidentiality, integrity, and availability of information. ISRM processes have been described in numerous standards and scientific work alike (Whitman & Mattord, 2014), (ISO/IEC 27001, 2013), (Siponen & Willison, 2009), each developed to meet its particular need with different objectives and activities (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016). However, this has also led to some confusion regarding the meaning of ISRM (Gerber & von Solms, 2005), and many, subtly different, definitions of its activities (Pan & Tomlinson, 2016). For example, a common ISRM standard such as ISO/IEC 27005 (2013) includes context establishment, risk assessment, risk treatment, and risk monitoring and review in its ISRM process, with various additional sub-activities. Another example is NIST SP 800-30 (NIST SP 800-30, 2012) in which the process consists of risk framing, risk assessing, risk response, and risk monitoring. While authors such as Spears and Barki (2010) describe the ISRM process as consisting of identifying and prioritising risk and implementing and monitoring controls. Whereas others such as Straub and Welke (1998) describe the process as consisting of activities to recognise security problems, perform risk analysis, generate security control alternatives, decide on security controls, and implement the selected security controls.

Although various ISRM processes differ in scope, depth and particular activities, they usually share some common goals like the identification and valuation of assets, analysis of risks, and the treatment of risks to reach an acceptable level (Visintine, 2003), (Shedden et al., 2010), (Whitman & Mattord, 2013), (Baskerville, Spagnoletti, & Kim, 2014). Therefore, ISRM in this study is described as giving a general view and structure, not adhering to any particular standard or process and being comprised of asset valuation, risk analysis, and selection of security controls. These have also been recognised as the basic ISRM activities (Saleh & Alfantookh, 2011).

However, for many ISRM processes, it is common that their activities are often described as if performed in a predominantly instrumental fashion (Lundgren & Bergström, 2019a). In this approach, each activity produces

particular outputs, which serves as input for the next (Wangen, Hallstensen, & Snekkenes, 2018). For example, the activity of asset valuation aims to identify and evaluate information assets and is often seen as a critical first step to risk analysis (Shameli-Sendi et al., 2016), and a cornerstone of information security since it helps prioritise security efforts (Wangen et al., 2018). In this activity, assets, tangible or intangible, that are valuable to the organisation are noted down with corresponding qualitative or quantitative valuation appraisement (Shameli-Sendi et al., 2016).

For each of these assets, a risk analysis is performed to identify and evaluate risks based on an estimation of vulnerabilities in systems and environments, the likelihood of a particular threat exploiting those vulnerabilities, and the criticality of the assets (Gerber & von Solms, 2005). The output of the risk analysis, in the form of the resulting estimations, is thus a first step towards selecting adequate security controls. It provides an overview of threats likely to affect assets integrity, availability and confidentiality, and the resulting impact thereof (Shameli-Sendi et al., 2016). As such, it is what enables rational decisions regarding what risks to treat. Basing the risk treatment decision without such insight could otherwise lead to high costs in terms of more expensive security controls than actually necessary, misdirected efforts, and loss of assets. In this fashion, security risks towards information assets are often portrayed as something that can be controlled, if managed rationally (Coles-Kemp, 2009), (Dhillon & Backhouse, 2001), (Lundgren & Bergström, 2019a).

In addition, it is also common to include some form of feedback operation that carries historical risk mitigation data, such as incidents, back to the previous activities to continuously improve the level of protection and threat relevance (Ahmad, Hadgkiss, & Ruighaver, 2012), (Webb, Ahmad, Maynard, & Shanks, 2014). As such, ISRM is a continuous process, and organisations which do not regularly perform its activities may risk consequences, such as direct financial impact, loss of reputation, or legal issues (Shameli-Sendi et al., 2016).

2.2 Information Security Risk Management Tools

Although there exists numerous ISRM processes, managing information security risks face many challenges because of the complexity and uncertainty involved in translating processes into actual practices. Indeed, many processes are only described in terms of what activities should exist, but not their content (Siponen, 2006).

Over the years, however, several tools have been developed to aid in this matter, and much effort has gone into identifying and help select among different ISRM tools. For example, Sajko, Hadjina, and Pešut (2010) used the Analytic Hierarchy Process (AHP) to establish a model for assisting the selection of a suitable ISRM tool. Gritzalis et al. (2018) similarly developed comparison criteria to better understand how ISRM tool's characteristics and methods could fit different organisation's needs. While agencies, like the European Union Agency for Cybersecurity (ENSIA), has compiled and maintains an inventory of ISRM tools (ENISA, 2019). Common for many of the tools concerned, is that they are designed to conform with particular standards and their respective activities and which are outlined in a series of steps to be followed (Gritzalis et al., 2018). Such tools could thus aid practitioners lacking the necessary experience and knowledge to interpret and translate ISRM processes into actual, practical activities.

However, the assistance of tools, while reassuring at first glance, could be a double-edged sword. For example, while the implied order of activities often found in research and standards can provide a valuable frame of reference regarding ISRM implementation, it could stifle organisational flexibility and fit if interpreted as a blueprint of reality (Lundgren & Bergström, 2019a). This is further amplified by ISRM tools designed to serve as guidance for activities, which could give the perception that the activities are static and not dynamic. Moreover, tools can only help so much. Ultimately, tools depend on the input data captured and provided by the practitioner, alongside their understanding of definitions and requirements, which have often proven to be too technical or ambiguous for the security-novice (Wangen, 2017). For example, both standards and tools often fall short in answering fundamental questions like how to perform this data collection, what counts as critical and non-critical assets, or how the likelihood of a threat can be estimated (Wangen, 2017), (Shameli-Sendi et al., 2016).

Furthermore, tools sometimes come with certain design restrictions or limitations, which can burden future ISRM developments. For example, in their meta-study on ISRM tools, Gritzalis et al. (2018) found examples of restrictive limits of characters allowed to be entered and saved in the tool, which could lead to useful data being undocumented and lost. Yet, human motivational elements are mostly neglected (Wangen et al., 2018), and many tools thus require good, or even expert, experience and knowledge to be used (Gritzalis et al., 2018). However, considering that it is often the on-site personnel and security-novices who conduct ISRM, additional work is needed to develop tools and activities that can make ISRM more efficient

(Wangen, 2017). Otherwise, ISRM activities and tools designed to ease its conduction could result in the opposite and instead end up burdening the entire process and risk causing SRS.

2.3 Security-Related Stress

The research topic of stress is extensive (Ayyagari, Grover, & Purvis, 2011) even when looking specifically at the ICT field. In the ICT field, stress-related research has traditionally been directed at technostress, i.e., stress experienced by ICT professionals (Ayyagari et al., 2011; Ragu-Nathan, Tarafdar, Ragu-Nathan, & Tu, 2008). For instance, technostress has been used to describe the end-user stress caused by a workplace full of accelerating technology demands (Ayyagari et al., 2011; Tarafdar, Tu, & Ragu-Nathan, 2010).

Technostress builds on a model where technological characteristics, i.e. attributes or features of a particular ICT acts as a stressor to an individual causing different types of strain (Ayyagari et al., 2011). There are different responses to technostress that include psychological, physical, or behavioural strain responses (Salanova, Llorens, & Ventura, 2014). Since the concept of technostress was put forward at the beginning of the eighties, different definitions have been developed (Salanova et al., 2014). In this study, the concept of Security-Related Stress (SRS), as introduced by D'Arcy et al. (2014), is used as a lens to study how security-novice ISRM practitioners are affected by such stress. D'Arcy et al. (2014) describe the SRS concept as the stressful demands imposed explicitly by security requirements, where SRS is *"caused by internal or external security-related demands appraised as taxing one's cognitive resources or abilities"* (D'Arcy et al., 2014 pp. 288).

As technostress is arguably a broader concept than SRS, D'Arcy et al. (2014) describes three dimensions of stress considered relevant from an information security context; *overload*, *complexity*, and *uncertainty*. Technostress also includes the dimensions; *invasion* and *insecurity* (Ragu-Nathan et al., 2008; Tarafdar et al., 2010) but they were omitted by D'Arcy et al. (2014) because they could not be reasonably adapted and because of conceptual overlap when applied in a security context. For these same reasons, the two dimensions are therefore omitted from this study as well.

For each of the SRS dimensions, there are both *stressors* and *stress inhibitors*. As described earlier, the stressors are the creators of stress, i.e., security factors that create stress for employees participating in, e.g. security processes. The stress inhibitors are, on the other hand, means of reducing

the level of stress (Ragu-Nathan et al., 2008), i.e., factors that decrease stress for employees participating in security work. By drawing from the technostress work of Ragu-Nathan et al. (2008), the work of D'Arcy et al. (2014), and ISRM literature, the SRS dimensions can be further conceptualised. The respective SRS dimensions from an ISRM perspective are elaborated below.

Overload from a technostress perspective, describes situations where ICT forces users to work faster and longer (Ragu-Nathan et al., 2008). From an SRS perspective, D'Arcy et al. (2014) describes overload as stressors stemming from security-related requirements that increase the workload, adding additional pressure to their job duties. For ISRM practitioners, this includes, e.g., the specific requirements that come from the activities in the ISRM process, i.e., the asset valuation, the risk analysis and the selection of security controls. Each of these activities has different requirements depending on, e.g. what system or asset to value, and for example, Sajko, Rabuzin, and Bača (2006) as well as Ozkan and Karabacak (2010) argue that it is not always evident what assets to classify, and how to do it. Add to the obstacle that security requirements often are seen as laborious and an unnecessary overhead that hinders productivity (Goel & Chengalur-Smith, 2010), (Posey, Bennett, & Roberts, 2011) and that it is typical for many ISRM practitioners not to work exclusively with information security, then a problematic view arises. The underlying reason is that generally, ISRM participants often have other primary duties and participate in, e.g. an asset valuation because they can add a perspective of being the information producer, information custodian, or information consumer (ISACA, 2012). Combined, participation in ISRM activities such as valuation and risk analysis can add extra stress to their situation.

Complexity from a technostress perspective describes situations where ICT complexity leads to users feeling inadequate with regard to their skills, and that they are forced to spend time and effort in learning and understanding, e.g. terms and concepts (Ragu-Nathan et al., 2008). From an SRS perspective, complexity can be described as stressors stemming from complex security requirements that force ISRM practitioners to spend additional time and effort on understanding new security requirements (D'Arcy et al., 2014). The information security domain is full of security requirements, and examples include, e.g., checklists, tools, and documentation containing technical or information security jargon (Puhakainen & Siponen, 2010). When novice ISRM participants encounter such requirements, they are sometimes forced to halt and read-up in order to be able to make informed decisions. It is well-known that there are several

different standards for managing information security, and many more standards for different security controls (Sveen, Torres, & Sarriegi, 2009). One example is the ISO/IEC 27005 (2013) standard that has shown to be challenging for novices to read and grasp (Wangen, 2017). Hence, practitioners lacking the required knowledge would need to spend more time reading up on security, instead of other, perhaps more pressing, work tasks and thus causing stress.

Uncertainty from a technostress perspective describes situations where continuing ICT changes and upgrades make users unsettled and create uncertainty so that they are forced to constantly update themselves (Ragu-Nathan et al., 2008). From an SRS perspective, uncertainty can be described as stressors stemming from continually changing and updated security requirements facing organisations (D'Arcy et al., 2014). Examples of such new or changing requirements could be the result of internal processes, demanding changes to established work practices, new laws and regulations (D'Arcy et al., 2014), or demands put by outside parties such as customers and business partners (Dlamini, Eloff, & Eloff, 2009). Some recent examples of new security requirements from the European Union include, e.g., the introduction of The Directive on security of network and information systems (NIS) (2016) and the General Data Protection Regulation (2016). Other uncertainty stressors include, e.g., mandatory periodical security training, changes in security tools, and the constantly changing risks facing the organisation. ISRM practitioners facing the dynamics of changes are forced to continually adjust to new requirements, causing uncertainty, and in the end, stress.

3 RESEARCH APPROACH

The following research approach starts with an introduction on how the data collection was performed and how the data was analysed. This is followed by an account of how the validation was conducted.

3.1 Data collection and analysis

As the focus of this work is to investigate the enactment of information security risk management by novice practitioners, an interpretative case study was initiated following the advice from Braa and Vidgen (1999). The protocol for case studies developed by Yin (2003) was used as a guiding reference. Based on SRS and ISRM literature, an analytical SRS lens consisting of the three SRS dimensions with the corresponding stress inhibitor was developed.

A university-level commissioned ISRM education, educating public sector ISRM practitioners, were contacted in order to connect with novice ISRM practitioners. These practitioners were mainly people who had been made responsible for ISRM, such as Chief Information Security Officers (CISO), whilst the others had other senior roles in their respective organisations such as e.g. managing director. However, none of them had any prior practical ISRM experience or knowledge, and therefore regarded as security-novices. Based on an initial discussion with those responsible for the course, and the course participants, two public sector organisations were selected as study objects. The organisations, from here on labelled as Alpha and Beta, were selected because they agreed on giving access to their internal ISRM documentation, consisting of policies and procedures for the overall ISRM process, and the activities such as, e.g. the asset valuation. Furthermore, Alpha and Beta agreed on participating in observations, interviews, and to share their experiences with other course participants.

Alpha is owned by 39 Swedish municipalities and one regional council, and Beta is a medium-sized Swedish municipality. Alpha provides services critical for citizens, and Beta, as a municipality, provides many functions and maintains infrastructure critical to society. Both Alpha and Beta have in the last years been affected by new requirements coming from the GDPR and the NIS directive. Striving to achieve information security, both Alpha and Beta have chosen to implement an ISRM process but are still early in their respective processes.

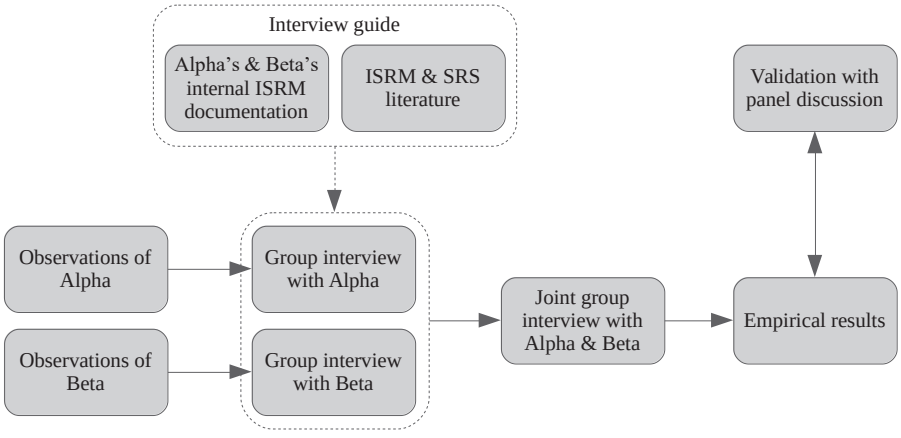


Figure 1. An overview of the research approach.

As a first step, both Alpha's and Beta's internal ISRM documentation, describing their approaches to valuation and risk analysis, were collected and analysed to get insights into their respective ISRM processes. The

analysis of the documentation, together with the dimensions of SRS formed the basis of the interview guide used for the open-ended questions encouraging the respondent to provide an extensive answer (Oates, 2006). An overview of the research approach can be seen in Figure 1.

The observations followed and were conducted for both Alpha and Beta in a series of workshops. Each workshop focused on a particular ISRM activity such as valuation or risk analysis and was led by a manager who was assigned as the workshop leader. These workshop leaders were themselves novices and participated in the ISRM education described above. The authors recorded everything with video and acted as complete observers, meaning that they took no part in the workshops (Oates, 2006).

Directly following the last observations, group interviews with Alpha and Beta were held, using the interview guide. The questions targeted clarifying questions, e.g., about their documentation practices, and more reflective questions about the enactment, such as *"what are your views on the valuation conducted today?"*, *"why did you participate in today's valuation?"*, or *"in your own words, how would you describe your experience with the ISRM process?"* To get more insights into the organisations' work practices, joint group interviews, including respondents from both Alpha and Beta, were held a few weeks after the observations. In this joint session, the managers who had participated previously in the observations and group interviews were invited. The nature of this joint group interview was to further elaborate on some aspects such as their views on the ISRM process, its activities, how tool usage affected them and compliance. An overview of the data collection can be seen in Table 1.

Table 1. An overview of the data collection.

Type of Data Collection	**Respondents and Quantity**	**Transcribed/ Collected**
4 observations	Alpha: 5 workshop participants Beta: 6 workshop participants 5 hours in total	7 pages
2 group interviews	Alpha: 5 respondents Beta: 6 respondents 1 hour and 15 minutes in total	2 pages
1 joint group interview	4 respondents from Alpha and Beta 1 hour	8 pages
1 validation	22 participants from 21 public sector organisations	7 pages
ISRM documentation	10 documents in total	76 pages

The observations and interviews were individual and partially transcribed by the authors, with a focus on the SRS dimensions. Other irrelevant data was omitted from the transcripts. For the data analysis, the SRS dimensions were used as predefined codes, i.e., overload, complexity, and uncertainty, together with each corresponding stress inhibitor. The data analysis was performed in three steps, based on qualitative content analysis (Cho & Lee, 2014). First, each author identified chunks of text in the transcripts corresponding to any of the codes. These chunks were then joined, sorted, and grouped based on the codes. Next, the authors examined the content of each code and extracted key concepts representing the codes jointly. Finally, each key concept was synthesised into a coherent text with associated descriptions.

3.2 Validation

In a paper on challenges in ISRM, Wangen and Snekkenes (2013) states that *"[o]ne of the biggest problems identified in the existing ISRM literature is the lack of validation"* (Wangen & Snekkenes, 2013 pp. 6). Similarly, Fenz and Ekelhart (2011) in their review on validation practices in ISRM, also stressed this point, and further reflected on the challenges related to knowing which validation approach to apply, and how. Generally, it is considered in qualitative approaches to take the results *"back to the people"*, i.e., to see if they conform to their own experiences (Silverman, 2015). In a similar manner to Fenz and Ekelhart's (2011) suggestion that an expert panel is an excellent approach to validate real-world ISRM parameters, a panel of novice practitioners were chosen to validate this particular case to see if the results conformed to their own experiences. In this case, the results were taken back to a new group of the university-level commissioned ISRM education, where none of the panel participants came from the organisations targeted in this study. The panel consisted of 22 information security managers from 21 public sector organisations. The panel discussion was held as a 1,5-hour long session where the results were presented and followed by a discussion. The session was recorded and transcribed.

4 EMPIRICAL RESULTS

The SRS dimensions, i.e., overload, complexity, and uncertainty, are each presented together with their corresponding stress inhibitors in separate sections. An overview of the empirical results is outlined in Table 2.

Table 2. An overview of the data collection.

SRS Dimension	Stressors and Stress Inhibitors
Overload stressors	– Tools promote sequential rather than agile workflow – Lacking time and resources to work with ISRM
Overload inhibitors	– Tools translating information value to security controls – The direct relation between information value and security controls was experienced as time-saving
Complexity stressors	– Mismatch in the language used in the ISRM documentation, the organisation and the tool – Too comprehensive ISRM documentation
Complexity inhibitors	– Walkthrough of the entire ISRM process to cover aims and objectives – Workshop leader preparing an embryo of possible information types to aid the start of the valuation
Uncertainty stressors	– External requirements (such as laws and regulations) – A mismatch between assumed work practices, ISRM documentation and use of tools – Lack of tool functionality, e.g., for documentation
Uncertainty inhibitor	– Workarounds in tool usage to fit work practices

4.1 Overload

The overload dimension was seen in both organisations in various forms, both as a part of the tools they used and the user's participation. Both organisations used existing tools and templates in varying degrees to help them perform and document the ISRM process. These were based on Microsoft Excel and Word and differed between the two organisations. Besides, both organisations used the same online tool, called "Klassa" (Sveriges Kommuner och Landsting, 2019), to help with the valuation. Klassa is a free-to-use Swedish public sector initiative aimed at supporting the ISRM process by helping to identify categories of potentially missing security controls, based on the information value and legal nature. Klassa is developed to support the valuation of systems containing assets, rather than the individual assets themselves, in an approach similar to the one described by Fibikova and Müller (2011). Based on the valuation of the system, the existing security controls, laws and regulations affecting the information in

the system, and the system itself, missing security controls are identified and serve as the output of the tool. Alpha finds that using a tool like Klassa alleviates the difficulty of translating information value to security controls, in effect acting as a stress inhibitor.

While both organisations used Klassa, the tool was perceived and used differently in two ways. First, the resulting list of categories of security controls was seen differently. In Alpha's case, the list represented a list of suggestions, and security controls to be addressed where needed. Alternatively, however, Beta, saw the result as a list of requirements to be implemented as is and not as categories of controls. Second, Alpha used Klassa as a support, and the result as they saw relevant: *"based on the items in this list, we must see 'are these relevant, or not?', but it is a great way to get started."* This aspect was similarly expressed during the panel discussion and could be seen as a stress inhibitor. During the panel discussion, it was recognised that the usage of tools gave a *"good foundation on which to stand on"* in order to reach a *"standardised view"* on the selection of security controls within the organisation. While Alpha saw Klassa as more of a support in their process, Beta centred their work process around it, which required several additional steps to import and export results between Excel and Klassa, in effect having Klassa shape their process rather than supporting it.

Beta's Excel tool was separated into different spreadsheets, one for valuation, one for the resulting list imported from Klassa, the third one for risk analysis, and a final one to put together a report. Each of these sheets were interlinked, serving as input and output for each other and thus promoting a sequential, rather than agile, workflow. Alpha's tool, on the other hand, did not dictate a particular workflow, allowing more agility. However, the workflow often implied in standards, inhibited them from adapting to situations more agilely. For example, one participant from Alpha recognised that they should not discuss risks during the valuation, i.e., by looking at the consequence rather than the likelihood. However, in the observation, it was clear that the workshop participants drifted into the risk analysis in order to land at a more correct valuation. At times, they would recognise that they were talking risks during the valuation, and discontinued their discussion, in effect discarding any identified risks since *"they [the risks] will be shown later in the risk analysis."* Later, during the group interview, one participant explained that it would benefit them to talk risks during valuation, since *"it comes as a natural step to think about risks during the valuation."*

One interesting aspect of using Klassa is that it provides a direct relationship between information value and security controls and does not necessarily decrease the workload. In Alpha's case, this relation informs their valuation, meaning that Alpha adjusts their valuation based on the consequential amount of security controls in which it would result. At one point, Alpha exclaimed that *"In the worst case, we might end up with a three [highest valuation level]"*, referring to the fact that a higher valuation will result in a more detailed list of security controls to consider than initially expected. In a similar attempt to decrease the workload, Beta encourages a rapid rather than precise approach, *"It is approximately 100 questions, so it is important to have tempo, tempo, tempo,... use your gut feeling."* In the joint group interviews, the long lists with questions posed by Klassa were discussed, and several suggestions on how to decrease the burden from a tool perspective were suggested by the respondents. For example, if the infrastructure is already valued and has received security controls accordingly, many questions in Klassa could be removed. Hence a more agile approach in the tool could decrease the time spent on the valuation.

In both Alpha's and Beta's cases, ISRM added stress to their daily work, since none of the participants in either organisation worked exclusively with security, and thus felt they had other, unrelated, work duties they needed to attend. For example, during the group interview when questioned about their opinions on finding security controls, one participant from Beta complained that *"well, this is not exactly the only thing we do"* in reference to participating in the ISRM process. Similarly, in Alpha's case, one participant explained that *"we cannot have a situation where our organisation gets affected by us sitting and doing risk analysis' all the time [...] perhaps it's a good thing during these major changes [the procurement of a new system]"* in reference to her participation in the ISRM process. In the joint group interview, lacking resources and time-saving measures were discussed, and one example that was emphasised was the direct relationship between information value and the security controls, or as one of the respondents put it *"by connecting information value to security controls... maximises [time utilisation]".* However, while the idea of not conducting a particular activity, or otherwise speed up its enactment, might at first sound like a stress inhibitor, maximising time utilisation. But on the other hand, it could also lead to more work, and in effect, act as a stressor instead. For example, during the panel discussion, it was mentioned that *"we only use the outcome [of the risk analysis], we don't save it, or take it further internally."* By not saving or sharing the outcome, threats and vulnerabilities justifying the security controls would remain undocumented, and unbeknownst to others in the organisation. Furthermore, similar

systems, future or already existing, which could have benefited from the analysis, would have to make their risk analysis from scratch, adding to the total work effort, and in effect, stress.

4.2 Complexity

To decrease complexity, both Alpha and Beta started their respective workshops with a walkthrough covering the aims and objectives of their entire ISRM process. This assisted in bringing the workshop participants up to speed on what to do and how to get started. Similarly, during the joint group interview, the respondents also reflected on this type of introduction as being an excellent way to introduce workshop participants and raise their awareness about the ISRM activities about to be conducted in the workshop. This was also reflected during the panel discussion. The panel agreed that, no matter the process, keeping practitioners informed with it would mean more efficient work, and less stress.

Despite this, during the observation, several indications were given by the workshop participants at Alpha and Beta about the difficulties in getting their respective ISRM cases started. For example, Alpha had a long discussion about their systems and information flow, trying to find a starting point for their valuation. This discussion was expected by the workshop leader, who had prepared a list of possible information types (e.g., customer data and log data) to be used as a starting point, despite lacking insights into the specifics of the systems. While this level of detail started a discussion on trying to identify correct information types, they, in the end, reached a valuation decision based on the system itself, rather than on all the discussed information types. In the interviews, the workshop leader was asked why this happened, and he replied: *"well, I must admit that I had them [the information types] in the back of my head during the process, and maybe we should have been more systematic valuing all the information types."* The motivation behind this was to get the discussions going. However, this also led to much information not being documented, for example, the motivation behind valuation decisions or various identified information types within the valued systems. This was expressed as a downside of Alpha's tool, *"you cannot really write any contextual information describing what the reasoning behind this valuation was"*, and as a result, had led them to create their separate document to carry such motivations. Although Alpha recognised that this added some additional time and complexity, they justified this by *"in the long run, it will be much easier to re-valuation in a year or two, to go back and see 'how did we think back then?'"* During the panel discussion, the participants similarly recognised the importance of documenting the process and the problems that arise when it is not done

correctly. An example was given regarding the valuation of existing systems versus valuation as a part of procurement. The valuation of existing systems was expressed as *"a nightmare… you don't wanna look under that rock,"* since such valuations led to the realisation of the lack of security controls, or that highly valued information existed in systems not adequately protected. It could also create a lot of extra work, trying to understand existing systems functionality, configuration or use. For example, it is not always easy, or even possible, to get hold of the required documentation, specifications, or personnel, inside or outside the organisation, with the necessary knowledge of the system being valued. Ultimately, forcing the practitioner responsible to spend much time trying to figure out the particular characteristics of a given system.

Beta, on the other hand, had difficulties not only in getting started but also in getting organisational acceptance of their ISRM approach. Beta's initial approach was in their words *"more complete"* and included a more comprehensive ISRM process. However, this approach *"was actively rejected by more or less everybody"* due to its comprehensiveness since it *"became far too extensive and complicated"*. As a result, Beta developed two additional, simplified, versions of the valuation to speed-up the ISRM process. However, this did little to help in practice, since choosing one of these simplified approaches was shown to be difficult, considering the selection itself depended on a firm understanding of the value of information. The respondents suggested that the primary motivation behind the three approaches was to stay compliant, *"doing something"*, rather than to increase security by having a sufficient ISRM process. During the panel discussion, a similar discussion arose about how to stay compliant. Here, the discussion was about ISRM standards, and how they could act as a complexity stressor, but also as a stress inhibitor, if applied more agilely to fit the organisations own pace. For example, it was discussed that standards, such as the ISO 27000 series, was too comprehensive to fully abide by, which seemed to discourage any idea of actually certifying their compliance. Instead, *"bits and pieces are extracted from the standard and applied to the organisation,"* to keep complexity at a reasonable level. In the joint group interview, the discussion went a bit further and suggested even more efforts in this regard could be decreased if security controls for specific information types, nationally or internationally, were standardised. Furthermore, it was discussed that certain types of systems have significant similarities regarding information types, and hence, tools could support information identification by giving examples of typical information types to decrease complexity.

Another aspect that was shown to cause complexity was the language barrier found in the tool use. The language in the tool Klassa, as the tool used by both Alpha and Beta, did not match the language used in their respective organisations, and during the observations, discussions halted several times so the workshop participants could discuss definitions of terms. Furthermore, at Beta, there were ambiguities in how to interpret the wording in Klassa, for example, discussions around what is included in *"measures to prevent and minimise operational disruptions are implemented"*, and *"technical and organisational measures are taken to manage identified risks."*

4.3 Uncertainty

In both Alpha's and Beta's cases, much of their ISRM work was externally motivated by the introduction of the NIS directive and GDPR, mandating a more systematic approach towards information security. During the observations, several indications were shown that suggested both organisations were in the early phases of establishing their processes. For example, the previously described direct relation between valuation and security controls, provided through the tool Klassa, was used as a stress inhibitor, since security controls for a particular information value are given. This was further discussed during the joint group interview, that it could be of help to have standardised security controls for a given type of information, covering both national and international requirements. However, this could also cause uncertainty, since the given set of security controls are externally defined, and in its nature, independent of context. For example, adapting to these, as is, could cause ambiguity in required security requirements. In Beta's case, one such example was the resulting security control *"Measures to prevent and minimise operational disturbances have been implemented"*, which was adopted into their risk analysis as is, and its security control noted as *"Do this"*.

Other indications were found in both organisations that suggested the early development of their respective ISRM processes. Their approach to the ISRM activities indicated a mismatch between assumed work practices, their policy and use of tools. For example, Alpha's template for documenting the valuation included procedures for how they should conduct a valuation, but these procedures did not correlate with their actual enactment. In practice, the tool did not support the flow of their work and discussions. Instead, it interrupted the workflow by having the workshop participants go back and forth in the tool to find the right sections. This focused much of their attention on the tool itself, rather than continuing and documenting their discussion. One example from Beta of how the tool

lacked in supporting their work process came when filling in a long checklist in Klassa. The workshop participants were advised to either ask colleagues for help, or in Klassa to fill in 'does not fulfil the requirement at all' if they were unsure about a question. Since all questions marked 'does not fulfil the requirement at all' will be tagged, it will work as a reminder in practice. The tool is not designed with any feature supporting saving questions to be discussed at a later stage, but it is needed, and hence a workaround is created. In the interviews, one of the respondents even reflected over this practice by stating that *"this feature 'does not fulfil the requirement at all' is very good, so you know where the gaps are."*

A mismatch between assumed work practice and the actual was similarly recognised during the panel discussion. However, it was further found that the awareness of having such misalignments was itself prone to act as a stressor. As one participant put it: *"it's difficult to admit that maybe we didn't follow the routines, especially if the boss is present in the meeting, and that maybe we are a bit uncertain [about the ISRM process]... this causes stress too."*

When it comes to the documentation of the ISRM work, both organisations acknowledged the lack of support from both the tool and their internal information management systems. The information saved in Klassa was deemed insufficient, as the reasoning behind decisions, generally expressed as contextual information, was not possible, and hence additional documentation was necessary. Both Alpha and Beta sent their ISRM documentation to their respective central organisational archiving functions. Alpha expressed that they *"do not have a great information management system"* and that by using their central archiving function, *"at least it is saved somewhere."*

5 DISCUSSION

While there is much research on what should be done with regard to ISRM, much of it has been shown to require a considerable amount of expertise to apply (Wangen, 2017), (Shedden et al., 2010). In this study, SRS (D'Arcy et al., 2014) was used as an analytical lens to investigate the enactment of ISRM by novice practitioners. It is reasonable to argue that SRS is a valid analytical lens to study novice practitioners, as a lack of security experience could cause overload, complexity and uncertainty. These dimensions of SRS gave additional insights into what challenges ISRM processes pose, which may not be evident for practitioners with more experience and could thus help in developing standards and tools to be more available for organisations perhaps not solely devoted to security issues. For example, our

findings point to the potential benefits and disadvantages of using tools to help perform various ISRM activities. Perhaps the most obvious is the experienced inflexibility in workflow and the inherent design of tools to support compliance, the difficulties in getting started, and limitations in what and how to document.

Throughout the observations, it was clear that the tools determined the ISRM process. Beta went so far as to design their work process around the online tool that they used. Although Alpha used the same online tool, they allowed for a more agile approach, but still seemed reluctant to do so, as if it would be wrong of them to perform ISRM activities in parallel, for example. An inadvertent gravitation, perhaps, towards including and conducting activities to ensure compliance with a particular standard. However, while it makes sense to perform ISRM activities chronologically, interpreting it as a blueprint of reality could burden the actual process enacted in practice, since it might not fit the current organisational context. Standards such as the ISO/IEC 27001 (2013) stress that the ISRM process should be adapted to the organisation. However, this adaption requires a certain level of experience, since standards are designed to be universal in scope and thus leave much to be interpreted by the practitioner. The resulting ambiguity is an example of an SRS complexity stressor.

During the panel discussion, standards were expressed as too comprehensive, resulting in much time and effort spent on understanding them. However, in order to overcome this complexity stressor, standards were adopted in smaller pieces, to ease the implementation and organisational fit, ultimately serving as a stress inhibitor. But at the same time, the adaptation of ISRM activities to organisational fit, could itself trigger stress in practice. Take Alpha for example; in their interpretation, risks ought not to be discussed during valuation, which resulted in them discouraging their discussion and leaving it undocumented, even though they exclaimed it could have helped them. In this example, the adaptation of activities into a natural workflow became an overload stressor. Adaption meant deviating from what otherwise was perceived to be the correct way of conducting the ISRM process. In effect, this discouraged a more effective workflow, and ultimately served as a stressor. In addition, the usage of tools, as an aid in interpreting and translating ISRM processes into actual, practical activities, seemed to have similar outcomes.

During the panel discussion, it was agreed that the assistance of tools could only help so much. In the end, tools still require the engagement and analysis on the part of the practitioner, to think outside the box, in order to

move forward. Indeed, the tools observed did not seem to help aid the workshop participants contextualising their ISRM process to fit the organisational needs. Instead, tools were seen as designed to strictly follow a pre-determined progression of ISRM activities. In effect, following the tools were interpreted as synonymous with being secure. This is consistent with Kwon and Johnson (2013), and Webb, Maynard, Ahmad, and Shanks (2016), who found that there is a growing misconception that compliance with formal processes is equivalent to good security. This was further seen in the case of Beta, which was motivated in their choice of methods as a means to stay compliant, rather than developing and adapting the ISRM process to tailor it to their organisational fit. In the joint group interview, compliance was discussed, and it was accepted that sometimes "good enough" (Bergström, Lundgren, & Ericson, 2019) is sufficient to cope with the SRS burden. That is, to know what level of abstraction is manageable in their context to reach compliance, rather than to get stuck in long discussions overdoing the level of details.

The limitations in knowing, deciding, and understanding what to document and how to document it was evident from the two cases. The tool Klassa lacked possibilities to add contextual information, e.g., the underlying motivations for the valuation and information on stakeholders handling the information, which is also an important input to the risk analysis. The transition from valuation to risk has proven troublesome (Sajko et al., 2006), (Ozkan & Karabacak, 2010), and the contextual information could potentially be more valuable than the actual valuation result at a future re-valuation (Lundgren & Bergström, 2019a). Lacking these possibilities, combined with a reluctance to save information in the cloud, meant that both organisations documented their ISRM results in various documents related to the valuation and risk analysis that in the end were sent to a central archive. These approaches inhibit the overall ISRM process as the results are fragmented, and an overview of all valued systems, identified risks and security controls are missing, which creates more work and could result in more SRS.

6 CONCLUSION

The purpose of this study was to explore security-novice practitioners' starting with ISRM and their enactment of its activities, using SRS as an analytical lens. It was found that studying novice ISRM practitioners from an SRS perspective highlighted the implications for research and standard developers alike. One such example were the mismatches in how standards are conceived and how they are interpreted in practice. This mismatch was further amplified by the tools supporting the ISRM process, both when

performing activities such as valuation, risk analysis and the selection of security controls but also when working with the overall ISRM process. For example, it was shown that tools could force the use of a particular process that was not aligned with the organisation, in effect stifling agility among the observed ISRM practitioners. The study further showed that design restrictions and limitations of tools could cause practical difficulties, such as the documentation of the ISRM process. In the observations, many of the difficulties related to documentation resulted not only in ad-hoc and inefficient practices but also in future developments such as the reuse of previous valuations of the same or similar information types, which otherwise could have been encouraged from a tool perspective.

This study also extends SRS research and shows that D'Arcy et al.'s (2014) SRS dimensions can be applied to the ISRM field. Understanding how SRS affects ISRM practitioners and how they are coping with SRS through various SRS inhibitors is essential and can help advance tool design, processes, and procedures related to ISRM. Several examples of SRS inhibitors were observed, e.g., the direct relation between valuation and security controls that provided a set of controls depending on the valuation is an example of such inhibitors. There are potentially several other SRS inhibitors related to the difficulties of identifying information types, and in deciding what to value, which better fitting tools could support.

This study indicates, by its in-depth approach in two organisations, and with the use of expert panel discussions, some future research issues that can be addressed. One such example is the sample size, and similar studies in a broader context could further build on the results presented here. Similarly, additional comparative studies of ISRM processes and tools are advised for further research and development. Finally, additional work is needed to better understand the challenges faced by novice practitioners and to help further develop standards and tools.

ACKNOWLEDGEMENT

This paper is a revised and expanded version of Lundgren and Bergström (2019b) presented at the 2019 International Conference on Cyber Science, 3-4 June 2019 in Oxford, UK. We want to thank the anonymous reviewers for their excellent suggestions and valuable insights.

7 REFERENCES

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident response teams – Challenges in supporting the organisational security function. *Computers & Security, 31*(5), 643-652. doi:https://doi.org/10.1016/j.cose.2012.04.001

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: technological antecedents and implications. *Mis Quarterly, 35*(4), 831-858.

Barrett, M., Davidson, E., Prabhu, J., & Vargo, S. L. (2015). Service innovation in the digital age: key contributions and future directions. *Mis Quarterly, 39*(1), 135-154. doi:10.25300/misq/2015/39:1.03

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

Bergström, E., Lundgren, M., & Ericson, Å. (2019). Revisiting Information Security Risk Management Challenges: A Practice Perspective. *Information and Computer Security, 27*(3), 358-372. doi:https://doi.org/10.1108/ICS-09-2018-0106

Braa, K., & Vidgen, R. (1999). Interpretation, intervention, and reduction in the organizational laboratory: a framework for in-context information system research. *Accounting, Management and Information Technologies, 9*(1), 25-47. doi:Doi: 10.1016/s0959-8022(98)00018-6

Broderick, J. S. (2001). Information Security Risk Management — When Should It be Managed? *Information Security Technical Report, 6*(3), 12-18. doi:https://doi.org/10.1016/S1363-4127(01)00303-X

Cho, J. Y., & Lee, E.-H. (2014). Reducing confusion about grounded theory and qualitative content analysis: Similarities and differences. *The Qualitative Report, 19*(32), 1.

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

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems, 31*(2), 285-318. doi:10.2753/MIS0742-1222310210

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153. doi:10.1046/j.1365-2575.2001.00099.x

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security, 28*(3), 189-198. doi:https://doi.org/10.1016/j.cose.2008.11.007

ENISA. (2019). Inventory of Risk Management / Risk Assessment Tools. Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools

Fenz, S., & Ekelhart, A. (2011). Verification, Validation, and Evaluation in Information Security Risk Management. *IEEE Security & Privacy, 9*(2), 58-65. doi:10.1109/MSP.2010.117

Fibikova, L., & Müller, R. (2011). A Simplified Approach for Classifying Applications. In N. R. Pohlmann, Helmut; Schneider, Wolfgang (Ed.), *ISSE 2010 Securing Electronic Business Processes* (pp. 39-49): Vieweg+Teubner.

General Data Protection Regulation. (2016). Regulation (EU) 2016/679. *Official Journal of the European Union, 119*, 1-88.

Gerber, M., & Solms, R. V. (2001). Special Features: From Risk Analysis to Security Requirements. *Comput. Secur., 20*(7), 577-584. doi:10.1016/s0167-4048(01)00706-4

Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers & Security, 24*(1), 16-30. doi:https://doi.org/10.1016/j.cose.2004.11.002

Gikas, C. (2010). A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. *Information Security Journal: A Global Perspective, 19*(3), 132-141. doi:10.1080/19393551003657019

Goel, S., & Chen, V. (2008). Can business process reengineering lead to security vulnerabilities: Analyzing the reengineered process. *International Journal of Production Economics, 115*(1), 104-112. doi:https://doi.org/10.1016/j.ijpe.2008.05.002

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

Gritzalis, D., Iseppi, G., Mylonas, A., & Stavrou, V. (2018). Exiting the Risk Assessment Maze: A Meta-Survey. *ACM Comput. Surv., 51*(1), 1-30. doi:10.1145/3145905

Gulati, R., & Soni, T. (2015). Digitization: A strategic key to business. *Journal of Advances in Business management, 1*(2), 60-67.

ISACA. (2012). *COBIT 5 Enabling Processes*. Rolling Meadows, IL.: ISACA.

ISO/IEC 27001. (2013). Information technology – Security techniques – Information security management systems – Requirements. In: ISO/IEC.

ISO/IEC 27005. (2013). *Information technology – Security techniques – Information security risk management*. Retrieved from

Kim, D. J., Yim, M.-S., Sugumaran, V., & Rao, H. R. (2016). Web assurance seal services, trust and consumers' concerns: an investigation of e-commerce transaction intentions across two nations. *European Journal of Information Systems, 25*(3), 252-273. doi:10.1057/ejis.2015.16

Kwon, J., & Johnson, M. E. (2013). Health-Care Security Strategies for Data Protection and Regulatory Compliance. *Journal of Management Information Systems, 30*(2), 41-66. doi:10.2753/MIS0742-1222300202

Labuschagne, L., & Eloff, J. H. P. (2000). Electronic commerce: the information-security challenge. *Information Management & Computer Security, 8*(3), 154-157. doi:doi:10.1108/09685220010372582

Lekkas, D., Katsikas, S. K., Spinellis, D. D., Gladychev, P., & Patel, A. (1999). User requirements of trusted third parties in Europe. *Proceedings, User identification and Privacy Protection Joint IFIP WG, 8*, 229-242.

Lundgren, M., & Bergström, E. (2019a). Dynamic Interplay in the Information Security Risk Management Process. *International Journal of Risk Assessment and Management, 22*(2), 212-230.

Lundgren, M., & Bergström, E. (2019b). *Security-Related Stress: A Perspective on Information Security Risk Management.* Paper presented at the 2019 International Conference On Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK.

NIST SP 800-30. (2012). *Guide for Conducting Risk Assessments*. Retrieved from Gaithersburg, MD:

Oates, B. J. (2006). *Researching Information Systems and Computing*. London: Sage.

Osborn, E., & Simpson, A. (2018). Risk and the Small-Scale Cyber Security Decision Making Dialogue—a UK Case Study. *The Computer Journal, 61*(4), 472-495.

Ozkan, S., & Karabacak, B. (2010). Collaborative risk method for information security management practices: A case context within Turkey. *International Journal of Information Management, 30*(6), 567-572. doi:http://dx.doi.org/10.1016/j.ijinfomgt.2010.08.007

Pan, L., & Tomlinson, A. (2016). A systematic review of information security risk assessment. *International Journal of Safety and Security Engineering, 6*(2), 270-281.

Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security, 30*(6), 486-497. doi:https://doi.org/10.1016/j.cose.2011.05.002

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly, 34*(4), 757-778.

Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., & Tu, Q. (2008). The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation. *Information Systems Research, 19*(4), 417-433. doi:10.1287/isre.1070.0165

Sajko, M., Hadjina, N., & Pešut, D. (2010, 24-28 May 2010). *Multi-criteria model for evaluation of information security risk assessment methods and tools.* Paper presented at the The 33rd International Convention MIPRO.

Sajko, M., Rabuzin, K., & Bača, M. (2006). How to calculate information value for effective security risk assessment. *Journal of Information and Organizational Sciences, 30*(2), 263-278.

Salanova, M., Llorens, S., & Ventura, M. (2014). Technostress: The Dark Side of Technologies. In C. Korunka & P. Hoonakker (Eds.), *The Impact of ICT on Quality of Working Life* (pp. 87-103). Dordrecht: Springer Netherlands.

Saleh, M. S., & Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management. *Applied Computing and Informatics, 9*(2), 107-118. doi:http://dx.doi.org/10.1016/j.aci.2011.05.002

Schirrmacher, N.-B., Ondrus, J., & Tan, F. T. C. (2018). *Towards a Response to Ransomware: Examining Digital Capabilities of the WannaCry Attack.* Paper presented at the Proceedings from PACIS.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security, 57*, 14-30. doi:https://doi.org/10.1016/j.cose.2015.11.001

Shedden, P., Smith, W., & Ahmad, A. (2010). *Information security risk assessment: towards a business practice perspective*. Paper presented at the Australian Information Security Management Conference 2010.

Silverman, D. (2015). *Interpreting qualitative data*: Sage.

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

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

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *Mis Quarterly, 34*(3), 503-522.

Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *Mis Quarterly, 22*(4), 441-469. doi:10.2307/249551

Sveen, F. O., Torres, J. M., & Sarriegi, J. M. (2009). Blind information security strategy. *International Journal of Critical Infrastructure Protection, 2*(3), 95-109. doi:https://doi.org/10.1016/j.ijcip.2009.07.003

Sveriges Kommuner och Landsting. (2019). Informationsklassning och handlingsplan [Information classification and action plan]. Retrieved from https://klassa-info.skl.se/

Tarafdar, M., Tu, Q., & Ragu-Nathan, T. S. (2010). Impact of Technostress on End-User Satisfaction and Performance. *Journal of Management Information Systems, 27*(3), 303-334. doi:10.2753/MIS0742-1222270311

The Directive on security of network and information systems (NIS). (2016). Directive (EU) 2016/1148. *Official Journal of the European Union, 194*, 1-30.

Wangen, G. (2017). Information Security Risk Assessment: A Method Comparison. *Computer, 50*(4), 52-61. doi:10.1109/mc.2017.107

Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness. *International Journal of Information Security, 17*(6), 681-699. doi:10.1007/s10207-017-0382-0

Wangen, G., & Snekkenes, E. (2013). *A taxonomy of challenges in information security risk management.* Paper presented at the Proceeding of Norwegian Information Security Conference/Norsk informasjonssikkerhetskonferanse-NISK 2013-Stavanger, 18th-20th November 2013.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security, 44*, 1-15. doi:https://doi.org/10.1016/j.cose.2014.04.005

Webb, J., Maynard, S. B., Ahmad, A., & Shanks, G. (2016). Foundations for an Intelligence-driven Information Security Risk-management System. *JITTA: Journal of Information Technology Theory and Application, 17*(3), 25.

Whitman, M. E., & Mattord, H. J. (2013). *Management of information security* (Fourth Edition ed.). Stamford, CT: Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2014). *Principles of Information Security* (Fifth ed.): Cengage Learning.

Visintine, V. (2003). An introduction to information risk assessment. *SANS institute, 8*.

Yin, R. (2003). *Case Study Research : Design and Methods* (Third ed.): Sage Publications.

KEY TERMS

Information Security Risk Management (ISRM): The continuous process of monitoring, identifying and valuing an organisation's information assets, and to analyse potential security risks against these assets in order to make informed decisions about what risks to mitigate, and what risks to accept.

Security-Related Stress (SRS): Stress caused by internal or external security-related requirements and demands which are experienced as

burdensome, complex, or ambiguous. In this study, SRS refers to three dimensions: overload, complexity, and uncertainty.

Stressor: The stressors are the creators of stress. From an SRS perspective, this is the security factors that create stress for employees participating in, e.g. security processes.

Stress inhibitor: The stress inhibitors are a means of reducing the level of stress. From an SRS perspective, these are the security factors that decrease stress for employees participating in, e.g. security processes.

Tools: Tools refer to aids aimed at assisting in the ISRM process. Tools can, therefore, take many shapes, including, but not limited to, such means as worksheets, document templates, or software designed to elaborate on the activities within the ISRM process.

BIOGRAPHICAL NOTES

Erik Bergström is a lecturer and PhD candidate at the School of Engineering at Jönköping University, Sweden. His main research interest lies in the field of information security management with a focus on information classification practices.

Martin Lundgren is a PhD candidate in Information Systems at Luleå University of Technology, Sweden. He received his BSc in Informatics from University of Gothenburg Sweden in 2012, and his MSc in Information Security from Luleå University of Technology in 2014. His general research interests are information security and risk management from socio-organisational perspectives.

REFERENCE

Reference to this paper should be made as follows: Bullo, A., Stavrou, E. & Stavrou, S. (2017). Transparent password policies: A case study of investigating end-user situational awareness. *International Journal on Cyber Situational Awareness*, Vol. 4, No. 1, pp128-154.