This is the published version of a paper published in .

Citation for the original published paper (version of record):

Stress Amongst Novice Information Security Risk Management Practitioners
https://doi.org/10.22619/IJCSA

Access to the published version may require subscription.

N.B. When citing this work, cite the original published paper.

https://creativecommons.org/licenses/by/4.0/legalcode

Permanent link to this version:
http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-18925
Stress Amongst Novice Information Security Risk Management Practitioners

Erik Bergström¹ and Martin Lundgren²

¹Department of Computer Science and Informatics, School of Engineering, Jönköping University, Jönköping, Sweden
²Department 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.
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, Gladychiev, & 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,
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.

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>
<thead>
<tr>
<th>Type of Data Collection</th>
<th>Respondents and Quantity</th>
<th>Transcribed/Collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 observations</td>
<td>Alpha: 5 workshop participants Beta: 6 workshop participants 5 hours in total</td>
<td>7 pages</td>
</tr>
<tr>
<td>2 group interviews</td>
<td>Alpha: 5 respondents Beta: 6 respondents 1 hour and 15 minutes in total</td>
<td>2 pages</td>
</tr>
<tr>
<td>1 joint group interview</td>
<td>4 respondents from Alpha and Beta 1 hour</td>
<td>8 pages</td>
</tr>
<tr>
<td>1 validation</td>
<td>22 participants from 21 public sector organisations</td>
<td>7 pages</td>
</tr>
<tr>
<td>ISRM documentation</td>
<td>10 documents in total</td>
<td>76 pages</td>
</tr>
</tbody>
</table>
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 “one 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.

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

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.


doi:https://doi.org/10.1016/j.im.2013.11.004


**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**