Received 12 March 2021
Revised 10 June 2021
31 July 2021
Accepted 1 August 2021

From rationale to lessons learned in the cloud information security risk assessment: a study of organizations in Sweden

Ana Faizi
Department of Computer Science, Information Systems, Luleå University of Technology, Luleå, Sweden, and
Ali Padyab and Andreas Naess
School of Informatics, University of Skövde, Skövde, Sweden

Abstract

Purpose – This study aims to address the issue of practicing information security risk assessment (ISRA) on cloud solutions by studying municipalities and large organizations in Sweden.

Design/methodology/approach – Four large organizations and five municipalities that use cloud services and conduct ISRA to adhere to their information security risk management practices were studied. Data were gathered qualitatively to answer the study's research question: How is ISRA practiced on the cloud? The Coat Hanger model was used as a theoretical lens to study and theorize the practices.

Findings – The results showed that the organizations aimed to follow the guidelines, in the form of frameworks or their own experience, to conduct ISRA; furthermore, the frameworks were altered to fit the organizations' needs. The results further indicated that one of the main concerns with the cloud ISRA was the absence of a culture that integrates risk management. Finally, the findings also stressed the importance of a good understanding and a well-written legal contract between the cloud providers and the organizations using the cloud services.

Originality/value – As opposed to the previous research, which was more inclined to try out and evaluate various cloud ISRA, the study provides insights into the practice of cloud ISRA experienced by the organizations. This study represents the first attempt to investigate cloud ISRA that organizations practice in managing their information security.

Keywords Cloud computing, Practice, Impact, Rationale, Information security risk assessment, Lesson learned

Paper type Research paper

Introduction

Cloud solutions have been firmly embedded into the fabric of many organizations. Research shows steady and remarkable growth in the implementation of cloud solutions (Paxton, 2016) owing to the benefits that they bring in areas such as cloud storage, enterprise cloud and mobile cloud. Organizations can benefit from high dynamic expansibility, virtualization

Information & Computer Security
Vol. 30 No. 2, 2022
pp. 190-205
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-03-2021-0034

with a large scale, high availability, use on-demand and payment by use offered by the cloud computing (Wang and Mu, 2011).

However, cloud solutions come with a cost regarding security and privacy (Hashizume *et al.*, 2013; Khan, 2016) that affect the organizational adoption of cloud solutions (Ali *et al.*, 2020; Kajiyama *et al.*, 2017). One of the reasons for security risks than in the traditional on-premises solutions lies in the outsourcing aspect, i.e. a third party is being trusted for managing the data. Another cause for concern is the multi-tenancy, wherein the resources are shared with other organizations through a wide network (Paxton, 2016). In this regard, resources being shared poses a further threat to the confidentiality and integrity of the data, and therefore, raise concern on data leakage (Wahlgren and Kowalski, 2013). A report by Cybersecurity Insiders (2018) reveals that the area causing the most concern is data loss and leakage, followed by data privacy and breach of confidentiality. The report also reveals that 84% of the information technology (IT) personnel did not think that traditional on-premises security solutions could be applicable on the cloud, and even if they did, they were thought to be limited (Cybersecurity Insiders, 2018).

Many information security risk management (ISRM) models have been developed and used for addressing security issues within the cloud (Albakri *et al.*, 2014; Islam *et al.*, 2017; Zhang *et al.*, 2010). Within ISRM resides the information security risk assessment (ISRA), which is a process that is integral to ISRM and its task is to identify, analyze, categorize and evaluate cloud security risks (Shameli-Sendi *et al.*, 2016). While plenty of ISRA frameworks exist for the cloud (Akinrolabu *et al.*, 2019; Djemame *et al.*, 2016; Islam *et al.*, 2017), extant research has tended to investigate the technical and operational issues (Venters and Whitley, 2012). Moreover, there is a lack of organizational perspective into cloud security issues (Trigueros-Preciado *et al.*, 2013), and previous research has called for more empirical studies that investigate the practice of ISRA in the cloud (Ali *et al.*, 2020). Thus, this research proposes the following research question that guides this study: *how do practitioners in the organizations conduct ISRA on cloud-based solutions?* This study aims to raise the understanding of practitioners' perspectives for assessing information security risks associated with the cloud. To answer the research question, the authors conducted a case study of cloud ISRA within four large organizations and five municipalities in Sweden through a series of in-depth interviews with the experts who conduct ISRA on a routine basis. The results of this research will help future research to theorize about the influences of practitioners in conducting cloud ISRA. From a practical perspective, this study portraits a rich picture of the practitioner's perspective that has been lacking in the cloud security literature.

This research paper is organized as follows. First, the paper provides a background of the study's main concepts related to security, cloud computing and ISRA. Second, the theoretical framework of the study is explained. This is followed by the description of the research methodology. Next, the paper presents the qualitative findings of the study. Further, we discuss the contributions of the results, including implications for the research, practice and education, as well as limitations and directions for future research.

Background

Information security risk assessment

The trend in information systems (IS) shows that it could be very costly if valuable information were compromised due to a breach in the systems. Therefore, the concept of risk is defined as the possibility of a compromising event occurring that will impact the IS. Risk is measured in terms of consequence (or impact) and the likelihood of the event. In this regard, a well-constructed risk assessment approach is a strategic tool for management decisions. While many ISRA models and frameworks exist, they fail to identify all the areas in which potential

vulnerabilities exist (Wangen, 2017; Wangen *et al.*, 2018). Therefore, no ISRA method is complete in itself, and a tweak and twist of the methods is a common activity.

One literature gap is related to the lack of practical research within organizations implementing ISRA; instead, the focus has been on the ISRA models and frameworks (Fulford, 2017; Siponen, 2006) with performed activities in a rational and predominantly instrumental fashion that do not reflect the reality (Lundgren and Bergström, 2019). One primary deficiency in the ISRA implementations includes information security risks that are commonly estimated with little reference to the organization's actual situation (Webb *et al.*, 2016). One reason for this gap is the difference between practitioners vs academic-based approaches to implement ISRA: "this will bring the academic methodologies closer in their application to the practitioner ones, though there will still be significant differences in the ways those two groups approach implementing technology risk management systems" (Fulford, 2017, p. 166). In this regard, extant research is mainly based on the researcher's opinions (Parker, 2007; Utin *et al.*, 2008) or the researcher's evaluation of ISRA frameworks and models as a proof of concept (Rajbhandari and Snekkenes, 2013; Shedden *et al.*, 2016), which are often disconnected from practitioner's perspectives. The current article fills this gap by investigating how practitioners theorize and learn by conducting ISRA.

Cloud computing and information security risk assessment approaches for the cloud

Cloud computing refers to a model for enabling ubiquitous, convenient and on-demand network access to the dynamically configured resources and delivering services in a scalable manner (Mell and Grance, 2011). Cloud computing is rapidly growing owing to the economic benefits it provides and the scalability it offers. The resources can be requested on-demand, which enhances the allocation of resources and decreases the losses that the extravagant resources may contribute to (Marston *et al.*, 2011). According to Statistics Sweden, cloud services in Swedish enterprises increased from 33% to 42% between 2016 and 2018 (SCB, 2018).

There are literature survey studies published, which are focused on the comparison of cloud risk assessment approaches. The works of Alturkistani and Emam (2014), Alosaimi and Alnuem (2016) and Drissi *et al.* (2016) present state of the art in cloud ISRA, which falls into three categories, namely, generic (i.e. not specific to cloud deployments), adaptations (i.e. customized from the generic standards) and specifically designed for the cloud. Despite the research prescribing approaches to conduct ISRA in the cloud, there is a lack of studies on how ISRA, in general, is practiced by the practitioners, let alone on the cloud (Fulford, 2017). Such lack of focus has been associated with the research gap between formal processes and those used in practice, i.e. the actual processes are shaped within the enactment of day-to-day activities and their respective challenges (Niemimaa and Niemimaa, 2017; Njenga and Brown, 2012; Webb *et al.*, 2016). Previous attempts to tackle the abovementioned research gap have been focused on training (Alshaikh *et al.*, 2018), capabilities (Lundgren, 2020; Wangen, 2017), organizational requirements (Ali *et al.*, 2020) and challenges (Bergström *et al.*, 2019; Fenz *et al.*, 2014) in the ISRA. Moreover, state-of-the-art research has mainly paid attention to on-site ISRA rather than cloud environment. It is needless to emphasize that the cloud environment has some unique characteristics, which cannot be exclusively studied from the traditional ISRA perspective (Albakri *et al.*, 2014; Rong *et al.*, 2013). Moreover, there is a lack of reports on implementation and experimental results that focus on cloud risk assessment (Theoharidou *et al.*, 2013).

The current study adds to the existing information security literature by investigating how learning from conducting cloud ISRA is achieved in practice, as learning is realized in the real world context, evolves and it is when practitioners reflect in action.

Method

Conducting interviews was the most suitable approach for this research. We sought to understand the practice of cloud ISRA conducted by the practitioners, and therefore, both the context and their perspective were essential factors to consider. Moreover, the current study is of exploratory nature that deals with contemporary events and do not require control of the behavioral environment. For this reason, we investigated different organizations as cases of cloud ISRA.

Data collection

The interview is a distinguished qualitative data collection method that allows the researchers to capture such complex phenomena and experiences from the practitioners' narratives (Schultze and Avital, 2011). Brinkman and Kvale (2015) mention that interviews are a great tool to gain knowledge about people's views and practices that they adhere to, e.g. actual practices of cloud ISRA. A semi-structured interview protocol was developed based on open-ended questions because closed-ended questions may lead to specific predicted answers. The time spent on interviewing each organization was, on average, 45 min. The interviews were conducted in two phases. In the first phase, four information security officers who worked in large organizations were interviewed from January to February 2019. In the second phase, IT experts who were responsible in five municipalities within the Västra Götaland region in Sweden were interviewed from April until May 2020.

Theoretical framework

A large and growing body of literature has investigated method practice within organizations and the difference between "formalized methods" and "methods-in-action" (Dittrich, 2016; Fitzgerald, 1996). Addressing the divergence between methods and practice depends on "how practitioners are able to make sense of the method at hand, and it also depends on whether the method to be integrated actually fits with the situated contingencies of the practice it should support" (Dittrich, 2016, p. 23). Therefore, theorizing practice help to unravel the complexities of everyday practices and methods in use (Feldman and Orlikowski, 2011).

The quest for an analytical lens that could concretely help us understand the practice of cloud ISRA by the practitioners led us to consider the Coat Hanger model. In their article, Päivärinta and Smolander (2015) propose a model to assist the researcher who intends to study the application, impact and practical implementation of a method and theorizes about the practices. As shown in Figure 1, the model consists of four main concept categories (contextual factors, rationale, espoused vs actual practices and impacts) and theorizing about relationships between them. The model is iterative as it is used routinely. The Coat Hanger model was proposed for software development; however, the critical elements in the model do not indicate that the model may be used exclusively for software development practices. As the authors suggest, the model could serve as an analytical tool for development practices (e.g. ISRA) to analyze the initial rationales (e.g. to secure information stored in the cloud), the emerging impacts (e.g. security breaches) and the espoused practices in context (e.g. tailor practices to fit the context better). Subsequently, these steps in the Coat Hanger model served as the basis for designing the interview protocol.

Participants

In total, 10 practitioners within large organizations and municipalities were interviewed. The reason for this selection was that after contacting small/medium-sized companies, we realized that these companies often do not conduct any ISRA on their cloud solutions, as their services were usually limited to software as a service. Because several of the interviewees preferred

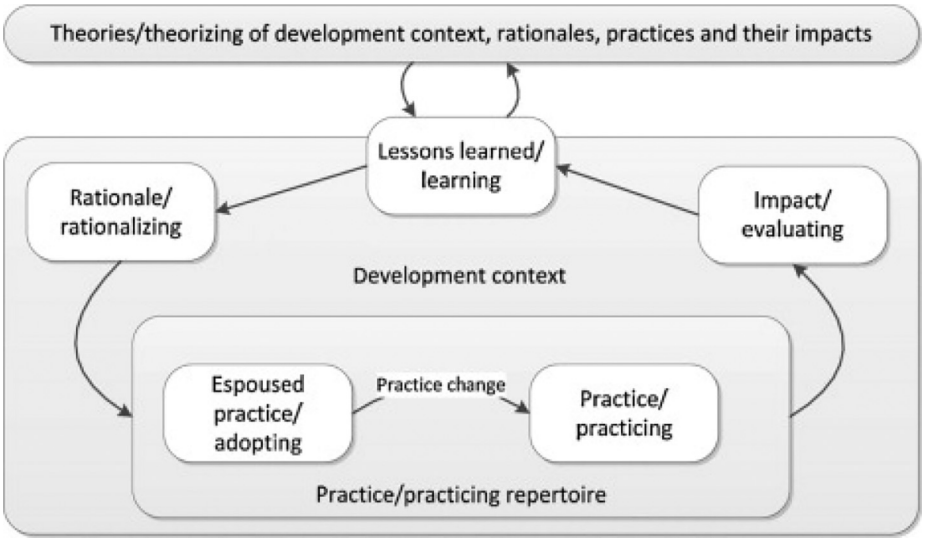

Figure 1.
Coat Hanger model for building theories from development practices (Päivärinta and Smolander, 2015)

anonymity, we present all practitioners and their organizations anonymously. Details about the practitioners' experience, role and organizations are illustrated in Table 1. Worthy of mentioning that two experts (Numbers 3 and 4) were working in the same organization.

Data analysis

All interviews were conducted via teleconferencing tools Skype and Zoom, recorded and transcribed verbatim. Qualitative content analysis was used for decoding the transcriptions, in which the concept categories of the Coat Hanger model as the analytical lens guided the deductive category application (Mayring, 2000). It is an iterative process where the coding of the data changes, either by combining, removing or renaming keywords used for the coding. First, the transcripts were thoroughly studied to determine "under what circumstances a text passage can be coded with a category" (Mayring, 2000, p. 164). Then the authors iteratively coded the interview transcripts according to the Coat Hanger model concepts (i.e. rationale, practice, impact and lessons learned). The focus of codes under each concept

Practitioner code	Organization type	Years of experience	Role
Expert 1	Private	+31	IT chief specialist
Expert 2	Private	+20	Chief information security officer
Expert 3	Private	+9	Information security leader
Expert 4	Private	+5	Information security officer
Expert 5	Private	+11	Cloud consultant
Expert 6	Municipality	+21	Information security officer
Expert 7	Municipality	+3	Information security specialist
Expert 8	Municipality	+4	Information security coordinator
Expert 9	Municipality	+5	Information security coordinator and data safety officer
Expert 10	Municipality	+20	Developer and administrator of information security services

Table 1.
List of participants

category was to determine the practices that the practitioners conduct during the process of cloud ISRA. Each code was compared to the previous codes, and in case of association with other, higher-order categories were created. In case of disagreements between the authors, collective discussions were made to reach a shared meaning of the content material to ensure the credibility of the findings (Lincoln and Guba, 1985). The authors found the amount of data reasonable when data saturation was reached (Tong *et al.*, 2007).

Results

The results from the analysis of the cases revealed that the organizations theorize about their ISRA cloud development practices. Below, the practices involved in each phase are presented in the light of the Coat Hanger model.

Rationale

According to the experts, the rationale for conducting ISRA in the cloud could be divided into general categories of complying with the external regulations and following internal ISRM frameworks. External requirements (e.g. compliance with the General Data Protection Regulation) is a driving force to conduct ISRA that usually deals with the critical practices that start with the questions such as "is this and that information critical to the business?" and "whether it requires protection?" In this regard, cloud provider's compliance with various laws is considered.

When it comes to the internal ISRM requirements, better business decision-making, identifying impact areas, how to influence the risks and using resources effectively with a balance between opportunity and risk tolerance were considered as the main rationales to conduct ISRA. Expert 5 explained their organization's rationale for conducting an ISRA as follows:

> *You have to mitigate risk; the only reason why risk analysis is done really is to mitigate the risks so that the resulting risk does not exist or is much lower than the original. (Expert 5)*

The frequency of practicing ISRA was depending on the services being transferred to the cloud. The level of organizational dependency on the cloud seemed to dictate when the risk assessment should be conducted. While some organizations had frequent routines (i.e. monthly and annually) to conduct ISRA, including the cloud, other organizations only conducted risk assessments when a solution was being launched to the cloud by addressing as many risks as early as possible to avoid surprises later on or when changes occurred. Information sensitivity is another initiator to determine how sensitive information assets are and if they can be stored on the cloud. Expert 3 mentioned that their ISRA team starts asking questions about the security risks with the introduction of a new cloud service:

> *What vendors are in question and what risks are connected to that specific vendor? [. . .] What type of integration are we talking about and what risks might arise from that integration? [. . .] (Expert 3)*

Practice

One finding was that the organizations relied on their experience and best practices to conduct the ISRA, although the level of integrating this internal knowledge application varied between the organizations. In some cases, the practice was based on experience and thoughts/ideas that had been gathered collectively throughout the years (e.g. through a knowledge base). In others, the formal ISRA models were modified based on the organizational needs in which some activities were removed (e.g. because they were too formal or too complicated), adapted to comply with the internal demand (e.g. rational) and had been simplified to comply with the organizations' capabilities:

> *This process is about compliance, compliance with our information security privacy standards and policies. We are deploying this process to give the tools to our business and our branches to do their own risk assessment. (Expert 4)*

Organizational influence on the practice of risk assessment existed in all cases, albeit with varying degrees. Level of freedom to determine the vulnerability level depended on the strategic governance of the organizations. In some cases, the board was involved with the decisions regarding cloud risks, such as whether certain information assets (e.g. documents) are allowed to be moved to the cloud, and the technical staff was appointed to assess the alternative solutions. In similar cases, a central unit was mainly responsible for conducting the risk assessments with close collaboration with the top management, whereas in some organizations, different units were responsible for conducting risk assessments independently. In some cases, however, depending on the complexity of the services and level of unit's maturity in conducting cloud ISRA, a central unit was available for assistance.

One interesting result was that the cloud characteristics led to deviations from the espoused practice to the actual practice, which led the organizations to contextualize the formal (sometimes non-cloud) ISRA frameworks (e.g. ISO/IEC 27005) because of enabled continuous learning and reflection-in-action from the practice. Some organizations reflected on this aspect because there were some features of the cloud, which in contrast to the on-premises, did not need to be in focus when conducting ISRA. These included that the on-premises servers had more monitoring authority and accessibility rights, whereas these rights were given to the cloud provider for the outsourced data; hence, risk related to the network structure did not have to be in focus for the cloud. In other cases, the organizations preferred to use platform as a service because they did not want to extend their data center to the cloud; yet, they still intended to use the desired functionalities of the cloud:

> *We use an incident-based method through an Excel template in which we determine what vulnerabilities can exploit this incident and then the likelihood and consequence [. . .] our [cloud ISRA] method was chosen because it is a normal risk assessment method and not too complicated [. . .] the method helps us in determining how the cloud service can be used. (Expert 9)*

Although all organizations acknowledged that trust in their cloud providers existed, they stressed that it should not be a blind one. The practices thus, considered cloud responsibility in addressing and assessing some security risks that exist within a cloud provider's environment. Therefore, all practitioners mentioned that a reference to their service level agreement (SLA) should be in place addressing the cloud provider's responsibility to protect their data.

Impact

Considering the initial rationale being compliant with internal and external ISRA requirements, most practices are believed to be in line with the rationale according to the practitioners. The impacts included making better business decisions, optimally using the resources, identifying the concerns by organizing meetings and keeping the staff updated with the newest threats. Throughout this process, some unexpected impacts occurred, which were affected by the practices. For example, in one case, the ISRA team decided to turn to the employees and ask them for risks they had encountered. This, however, resulted in a lack of participation and the burden of establishing routines regarding which security personnel ought to be contacted and how employees could get assistance was experienced. The impact was consequently unsatisfactory, resulting in the risks associated with daily employee activities being undetected. The experts recognized that some security countermeasures might be construed as a hindrance to some employees. Furthermore, they pointed out the importance of keeping the employees informed of information security risks:

[. . .] it also took a lot of time to get engagement from outside [of the ISRA team]; not everyone is equally happy to spend time every month looking at the risks and thinking what changed and what can be done about it. (Expert 2)

For some organizations, the speed of ISRA impacted the next round, as the risks that previously had already been identified would be known when ISRA is conducted next time. In this regard, the more the risk assessment occurred, the more rapid the assessments became because the one conducting the ISRA learned what to assess quickly.

With the introduction of a new service, sometimes the result of the risk analysis has given rise to new requirements specified during service level agreements negotiations with the cloud provider. A common tactic for dealing with threats and vulnerabilities was to determine security requirement specifications concerning the service level agreement, and thus, make sure that the service provider would match the desired level of security controls. In one municipality, the risk analysis led to the termination of their contract with the cloud provider that did not live up to the storage security requirements of that municipality:

I believe the security of the municipality has increased since risk assessment has been made [. . .] we have been better at specifying requirement during service level agreements and in making sure that cloud service is being used in a secure manner, such as what kind of information the employees are allowed to store in the cloud. (Expert 8)

Lessons learned

All interviewed organizations expressed that the previous cycle of ISRA affected the upcoming one and that they all revisited the previous risk assessment outcomes, including cloud-related risks in the annual risk assessment. Such lessons manifested into updating the ISRA frameworks throughout time.

Risk assessment has helped organizations recognize the expected risk of cloud services independent of the cloud services or provider. They have learned that they cannot entirely depend on the cloud service provider but have to become better at specifying requirements during negotiations. It has also helped them ask the right questions to get them involved parties into the right mindset. They wanted to avoid changing the method as it takes time to learn and opted instead to make minor adjustments to the method:

We try to avoid replacing our [cloud ISRA] method and instead opt to adjust the current method as we believe that risk assessment should be kept simple. (Expert 10)

Therefore, the ISRA approaches were constantly reviewed and evaluated to assess their effectiveness with regard to the security risks:

[. . .] of course, we are learning from our risks, we are learning how to define our risk landscape [. . .] so, when we do the risk assessment on the same solution, platform, or infrastructure, we review the previous assessment and the risks that were connected to that solution, and check that the risk has been mitigated [. . .]. (Expert 3)

A summary table of various elements for each step of the process is presented in Table 2 below:

Discussion

This research sought to understand the practice of cloud ISRA. The previous research has either studied cloud ISRA from the perspectives of those who have designed the artefacts via proof of concepts or superficial cases that lack nuances of cloud ISRA practice. This study, therefore, contributes to the cloud ISRA research by increasing our understanding of how practitioners conduct ISRA on the cloud. Through the lens of the Coat Hanger model, the

Rationale	• Why? – goal – To identify information assets and to determine, which information assets are affected by which cloud service – Compliance with laws and regulations • Avoid economic, reputation and legal consequences – Cost/benefit analysis of countermeasures – Serving as supportive material for other risk assessments (e.g. on-site) – Check if SLA with the cloud provider is achieved – To identify threats and vulnerabilities in the cloud – Cloud ISRA framework/method maturity • When? – initiation – Introduction of a new service – Changes in the current services – Interval varies between monthly to yearly and every three years • Each cycle typically lasts a couple of days to one week
Practice	• Who is involved? – Employees working with a specific cloud service – Information asset owners – IT department – Info security experts in the organization • Cloud ISRA frameworks/methods – No specific (e.g. a matrix with risk likelihood and consequences) – ISO/IEC 27000 series – Metodstöd (Swedish Civil Contingencies Agency) – KLASSA information classification method created by the Swedish Association of Local Authorities and Regions – Combined methods, e.g. ISO/IEC 27005 and Metodstöd – In-house (derived from other non-cloud ISRA frameworks) – Methods are either chosen based on the familiarity of those conducting ISRA with the method or inherited from before • Tracking information assets whether they reside on the servers inside the organization or the cloud • Trusting the cloud provider affects the scope of the assessment • Analyzing the technical architecture, if possible, however, there are limitations • Dealing with the entanglement of the root cause of the risks; whether the risks come from a process, routine and practice inside or if they are related to the cloud vulnerabilities

Table 2.
Summary of the results

(*continued*)

	• Increasing risk scope, and therefore, the risk should be viewed as widely as possible
	• Deciding which activities fall under the organization domain and which are cloud's responsibilities
	– Managing risks are a combination of technical and operational activities (e.g. raising employee awareness to report the risks and encryption of data stored on the cloud)
Impact	• The decision on whether to shut down a cloud service
	• Cyber situational awareness
	– Making business decisions and using the resources in an optimal way
	• Cloud ISRA makes the organizations better at specifying requirements during service level agreements
Lessons learned	• Overall security culture improved
	• Learning ISRA frameworks/methods
	• Organizations learn that they cannot entirely depend on the cloud service provider but must become better at specifying requirements during negotiations
	• Aligning overall security and cloud strategies
	• Cloud ISRA method adjustments are made after each iteration based on the alignment of assessed risks and ISRA rationale
	• A good cloud ISRA practice is both top-down and bottom-up, meaning that top management should support cloud ISRA and employees should be involved
	• Coordination of information security risks collected from different units and to propagate risk awareness in the whole organization

Table 2.

results suggest that the practice of cloud ISRA is a learning process in which there is an interplay with the contextual nuances (factors and rationale), practices (espoused and actual) and verified impacts in accordance with the ISRA rationale. Below we discuss the study's findings and theorize on the cloud ISRA practice.

Research within ISRA pointed to a mismatch between the espoused and the actual actions by the practitioners (Bergström *et al.*, 2019; Shedden *et al.*, 2016; Webb *et al.*, 2016). Those studies have focused on understanding the reasons behind such mismatch but not how practitioners theorize and learn by conducting ISRA. Our empirical results indicate that the rationale behind conducting ISRA leads to particular decisions on how it is practiced, and the practice is refined based on the impact of the risks. Arguing from a practice perspective, previous research has emphasized understanding the practitioner's rationalities of adopting methods (Dittrich, 2016; Feldman and Orlikowski, 2011). Our study showed that the rationale of ISRA practice impacts the choice of the method adopted and the extent to which such method supports the practitioner in the integration risk assessment goals. For

example, if the rationale of ISRA is only for compliance purposes, the choice of method and activities will be affected accordingly.

Our empirical data support the previous research by showing that formal textbook ISRA frameworks are regularly contextualized (Fenz *et al.*, 2014). Some studies have shown that abstract practices are translated from other contexts to local conditions (Backhouse *et al.*, 2006). This translation was evident in our study by meeting the challenges of coping with the context of practice (e.g. the dynamic nature of the cloud) and the rationale of the practice by using a non-specific cloud ISRA (e.g. ISO/IEC 27005). Consequently, the practice needs to accommodate such dynamic changes (e.g. information moving from one cloud service to another) because of which new rules and understandings evolve.

With respect to the lessons learned and theorization by the practitioners, our findings indicate the reflection-in-action thinking mode among cloud ISRA practitioners. In this mode, the practice is seen as a means in which the practitioner gains skill and mastery through refinements and using previous experiences rather than scientific theory and technique being applied during problem-solving (Päivärinta and Smolander, 2015). In our study, contextual learning and reflection-in-action manifested through the refinements (e.g. simplification) to an already used method rather than adopting a new method by the practitioners, which were studied, adjusted to lessen its complexity and altered to fit the organization's needs (Webb *et al.*, 2016).

Based on the theoretical lens adopted in this research and the empirical data on the practice of cloud ISRA, our research contributes to the information security field by illustrating that *the cloud ISRA is driven by the rationale of practice and accommodated in a way that the practitioners would be able to integrate their lessons learned into it.* We believe that the contribution has important implications for research, practice and education, as discussed below.

Implications for research

The findings of this study provide the following implications for research. First, this study highlights that the practice of cloud ISRA is a dynamic process that involves considerations for the rationale, practice (i.e. espoused and actual), impact and learning. This finding aligns with the previous research indicating flexibility as an essential factor from the practitioner's perspective (Padyab *et al.*, 2014). However, our study contributes to the information security research by providing a new understanding of the reasons behind demanding flexibility deemed rooted within the overall cloud ISRA theorization by the practitioners. Therefore, the implication is that a method to support cloud ISRA should have inherent flexibility.

Second, ISRA approaches are not static, which is contrary to the pre-supposition of most cloud ISRA approaches. The extent of development in cloud risk assessment models and frameworks (Akinrolabu *et al.*, 2019; Albakri *et al.*, 2014; Djemame *et al.*, 2016; Islam *et al.*, 2017) assume that the process is static and changes to the approach are not recognized, which is contrary to the results of the current paper. An implication for future research is to investigate whether the changes made by practitioners are effective or counter-effective. Another implication is to call for more research on approaches that tolerate changes to the ISRA methods. An interesting finding was that practitioners were inclined to use the traditional IT risk assessment frameworks, e.g. ISO/IEC 27005. A plausible explanation could be related to an unwillingness to learn a new method, method complexity, uncertainty or lack of documentation support from the methods (Bergström and Lundgren, 2019). This finding could be related to the "ease of use" factor, as practitioners preferred to apply standard approaches that are easier to use because they were used on-site rather than adopting a cloud-specific ISRA. The organizations in our study were using mainstream ISRA frameworks (e.g. ISO/IEC 27005, ISO/IEC 31000, The

Swedish Civil Contingencies Agency method support (MSB, 2018)) for compliance purposes. While previous research has argued that the traditional ISRA methods are not suitable for the cloud environment (Albakri *et al.*, 2014), the situation seems different in practice. We acknowledge that our data cannot represent the adopted cloud ISRA; however, it will be fruitful for future research to investigate why such a gap exists.

Third, the findings complement the previous literature on the challenges of ISRM (Bergström *et al.*, 2019; Fenz *et al.*, 2014) with nuances of the cloud context. Our study departs from those of Bergström *et al.* (2019) and Fenz *et al.* (2014), who studied challenges concerning the process of ISRA, by providing an alternative view of ISRA challenges in relation to the process of practice theorization. Through the lens of the Coat Hanger model, it can be argued that addressing the challenges of cloud ISRA by the practitioners is a cyclic learning process at different stages of the practice (refer to Figure 1 and Table 2). This contribution herein illustrates that mapping cloud ISRA challenges with the concept categories (rationale, espoused vs actual practices, impacts and lessons learned), similar to Table 2, will help researchers monitor at which stage the challenge occurs, how it is addressed, what new practice has emerged and how challenge and solution affect the other concept categories.

The fourth implication for research is to study the relationship between the ISRA done on the cloud and other methods, frameworks and models used in an organization. For example, developing a service hosted in a cloud environment needs particular precautions planned during its development lifecycle. In this regard, cloud ISRA must be considered for a secure deployment. Therefore, there should be constant integration between the software development lifecycle and cloud ISRA. We could not find any previous research that studies the interaction between ISRA and other organizational practices.

Implications for practice

This research reinforces the value assumption that professional reflection-in-action plays a vital role in information security management (Hedström *et al.*, 2011) and cloud ISRA flows within the same stream. In this regard, organizations should "establish vehicles for organizational learning, particularly by reducing discordance between espoused theories and theories in-use" (Dhillon, 2008, p. 300). We believe that our research gives a clear perspective on how practitioners could theorize about their practices with the help of a practice theorization model, i.e. the Coat Hanger model.

From a practical standpoint, the findings indicated a grey area between the infrastructure providers and organizations implementing, deploying and overseeing their services. While previous research has shown that organizations assess the cloud before committing to an SLA (Djemame *et al.*, 2016), our results showed that the organizations consider SLA an ongoing challenge, especially after each ISRA round. This practical challenge creates a dilemma where organizations deem that the existing risks are not covered in the SLA with the cloud provider. While solutions in the previous literature regarding the selection of cloud providers based on the desired SLA exists (Islam *et al.*, 2017; Luna *et al.*, 2015), there is no provision in the literature regarding the negotiation of security SLA after the migration to the cloud. Another interesting finding was related to SLA as a means to a risk mitigation strategy by the organizations. Previous research has indicated that SLAs are a significant, influential factor in cloud computing security (Ali *et al.*, 2020). While an SLA is usually negotiated before adopting cloud services by the organizations, our results suggest that organizations deal with the updates to the SLA after each round of cloud ISRA practice (i.e. theorizing from ISRA practice). The challenge is to choose whether

risk mitigation strategies should focus on the updates to the SLA. We suggest that the practitioners consider this issue during the cloud ISRA.

Implications for education

Understanding the challenges behind the identified cloud ISRA can help improve education and state-of-the-art methods in information security. Previous research has argued about the unfitness of traditional ISRA for the cloud (Albakri *et al.*, 2014), and despite such arguments, practitioners are more inclined to accommodate adopted (non-cloud specific) ISRA for the cloud. The tendency to accommodate traditional ISRA into the cloud should not be considered as counter-effective. However, ISRA practitioners must become aware of the deficiencies of the traditional ISRA applied to the cloud and customize their methods toward the cloud. In this regard, it is vital to educate the information security students as future security professionals on how to theorize about their practices to accommodate their adopted methods with the rationale of the ISRA. Moreover, in addition to understanding the main concepts of ISRA, reflection-in-action should form the basis for the method modification. Therefore, instructors should train students and practitioners to make changes to the practiced method grounded within rationale, practice, impact and theorization.

Limitations

The research did not intend to evaluate a specific model; instead, it looks at how ISRA is conducted for cloud solutions as a whole and we did not study each essential part such as risk identification, analysis and evaluation separately. All the organizations studied in this research are located in Sweden, and therefore, caution should be exercised in applying them to other contexts. Furthermore, it would be interesting to integrate cloud providers' perspectives into their customers' cloud ISRA practice. Moreover, we aimed to investigate the intended rationale for the actual realization and resulting impacts of cloud ISRA. The Coat hanger model was deemed suitable in this research; however, future research could integrate general practice theories and institutional theory as a theoretical lens.

Conclusion

In total, 10 IT security experts were interviewed to answer the question "how do organizations conduct cloud ISRA?" Analyzing the data through the used theoretical framework showed that the cloud ISRA is driven by the rationale of practice and accommodated so that the practitioners would be able to integrate their lessons learned into it. The study showed that the organizations focus on identifying information assets, mainly because it is vital to determine what information is being used by what service, as there is a certain lack of clarity when it comes to what is allowed to be stored on a cloud service. Some organizations opted to use SLAs to ensure that their information is handled with care. It seems the organizations currently lack a standardized approach for conducting ISRA and most of them want their ISRA method to be simple, meaning that the status quo cloud ISRA approaches may be too complex.

References

Akinrolabu, O., New, S. and Martin, A. (2019), "CSCCRA: a novel quantitative risk assessment model for SaaS cloud service providers", *Computers*, Vol. 8 No. 3, p. 66.

Albakri, S.H., Shanmugam, B., Samy, G.N., Idris, N.B. and Ahmed, A. (2014), "Security risk assessment framework for cloud computing environments", *Security and Communication Networks*, Vol. 7 No. 11, pp. 2114-2124.

Ali, O., Shrestha, A., Chatfield, A. and Murray, P. (2020), "Assessing information security risks in the cloud: a case study of Australian local government authorities", *Government Information Quarterly*, Vol. 37 No. 1, p. 101419.

Alosaimi, R. and Alnuem, M. (2016), "A survey on security risk management frameworks in cloud computing", *Computer Science and Information Technology (CS and IT)*, pp. 1-11.

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

Alturkistani, F.M. and Emam, A.Z. (2014), "A review of security risk assessment methods in cloud computing", in Rocha, Á., Correia, A.M., Tan, F.B. and Stroetmann, K.A. (Eds), *New Perspectives in Information Systems and Technologies*, Springer International Publishing, Cham, Vol. 1, pp. 443-453.

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 Quarterly*, Vol. 30, pp. 413-438.

Bergström, E. and Lundgren, M. (2019), "Stress amongst novice information security risk management practitioners", *International Journal on Cyber Situational Awareness*, Vol. 4 No. 1, pp. 128-154.

Bergström, E., Lundgren, M. and Ericson, Å. (2019), "Revisiting information security risk management challenges: a practice perspective", *Information and Computer Security*, Vol. 27 No. 3, pp. 358-372.

Brinkman, S. and Kvale, S. (2015), "Interviews: learning the craft of qualitative research interviewing", *Aalborg*, Vol. 24, p. 2017.

Cybersecurity Insiders (2018), "2018 cloud security report", *Cybersecurity Insiders*, available at: www.cybersecurity-insiders.com/portfolio/2018-cloud-security-report-download/ (accessed 28 April 2020).

Dhillon, G. (2008), "Organizational competence for harnessing IT: a case study", *Information and Management*, Vol. 45 No. 5, pp. 297-303.

Dittrich, Y. (2016), "What does it mean to use a method? Towards a practice theory for software engineering", *Information and Software Technology*, Vol. 70, pp. 220-231.

Djemame, K., Armstrong, D., Guitart, J. and Macias, M. (2016), "A risk assessment framework for cloud computing", *IEEE Transactions on Cloud Computing*, Vol. 4 No. 3, pp. 265-278.

Drissi, S., Benhadou, S. and Medromi, H. (2016), *A New Shared and Comprehensive Tool of Cloud Computing Security Risk Assessment*, in Sabir, E., Medromi, H. and Sadik, M. (Eds), Springer, Singapore, pp. 155-167.

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

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.

Fitzgerald, B. (1996), "Formalized systems development methodologies: a critical perspective", *Information Systems Journal*, Vol. 6 No. 1, pp. 3-23.

Fulford, J.E. (2017), "What factors influence companies' successful implementations of technology risk management systems?", *Muma Business Review*, Vol. 1 No. 13, pp. 157-169.

Hashizume, K., Rosado, D.G., Fernández-Medina, E. and Fernandez, E.B. (2013), "An analysis of security issues for cloud computing", *Journal of Internet Services and Applications*, Vol. 4 No. 1, p. 5.

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

Islam, S., Fenz, S., Weippl, E. and Mouratidis, H. (2017), "A risk management framework for cloud migration decision support", *Journal of Risk and Financial Management*, Vol. 10 No. 2, p. 10.

Kajiyama, T., Jennex, M. and Addo, T. (2017), "To cloud or not to cloud: how risks and threats are affecting cloud adoption decisions", *Information and Computer Security*, Vol. 25 No. 5, pp. 634-659.

Khan, M.A. (2016), "A survey of security issues for cloud computing", *Journal of Network and Computer Applications*, Vol. 71, pp. 11-29.

Lincoln, Y.S. and Guba, E.G. (1985), *Naturalistic Inquiry*, SAGE Publications.

Luna, J., Suri, N., Iorga, M. and Karmel, A. (2015), "Leveraging the potential of cloud security service-level agreements through standards", *IEEE Cloud Computing*, Vol. 2 No. 3, pp. 32-40.

Lundgren, M. (2020), "Rethinking capabilities in information security risk management: a systematic literature review", *International Journal of Risk Assessment and Management*, Vol. 23 No. 2, pp. 169-190.

Lundgren, M. and Bergström, E. (2019), "Dynamic interplay in the information security risk management process", *International Journal of Risk Assessment and Management*, Vol. 22 No. 2, p. 212.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A. (2011), "Cloud computing – the business perspective", *Decision Support Systems*, Vol. 51 No. 1, pp. 176-189.

Mayring, P. (2000), "Qualitative content analysis – research instrument or mode of interpretation?", in Kiegelmann, M. (Ed.), *The Role of the Researcher in Qualitative Psychology*, Tübingen, Huber, pp. 139-148.

Mell, P., Grance, T. (2011), "The NIST definition of cloud computing", *NIST Spec. Publ*, Vol. 800 Computer Security Division, Information Technology Laboratory, National . . ..

MSB (2018), "Metodstöd för systematiskt informationssäkerhetsarbete", available at: www.informationssakerhet.se/metodstodet/ (accessed 5 March 2021).

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, pp. 1-20.

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

Padyab, A.M., Päivärinta, T. and Harnesk, D. (2014), "Genre-based approach to assessing information and knowledge security risks", *International Journal of Knowledge Management (IJKM)*, Vol. 10 No. 2, pp. 13-27.

Päivärinta, T. and Smolander, K. (2015), "Theorizing about software development practices", *Science of Computer Programming*, Vol. 101, pp. 124-135.

Parker, D.B. (2007), "Risks of risk-based security", *Communications of the ACM*, Vol. 50 No. 3, p. 120.

Paxton, N.C. (2016), "Cloud security: a review of current issues and proposed solutions", *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*, pp. 452-455.

Rajbhandari, L. and Snekkenes, E. (2013), "Using the conflicting incentives risk analysis method", in Janczewski, L.J., Wolfe, H.B. and Shenoi, S. (Eds), *Security and Privacy Protection in Information Processing Systems*, Springer, Berlin, Heidelberg, pp. 315-329.

Rong, C., Nguyen, S.T. and Jaatun, M.G. (2013), "Beyond lightning: a survey on security challenges in cloud computing", *Computers and Electrical Engineering*, Vol. 39 No. 1, pp. 47-54.

SCB (2018), "Use of cloud services is increasing among enterprises", *Statistiska Centralbyrån*, available at: www.scb.se/en/finding-statistics/statistics-by-subject-area/business-activities/structure-of-the-business-sector/ict-usage-in-enterprises/pong/statistical-news/ict-usage-in-enterprises-2018/ (accessed 29 April 2020).

Schultze, U. and Avital, M. (2011), "Designing interviews to generate rich data for information systems research", *Information and Organization*, Vol. 21 No. 1, pp. 1-16.

Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. (2016), "Taxonomy of information security risk assessment (ISRA)", *Computers and Security*, Vol. 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*, Vol. 39 No. 1.

Siponen, M. (2006), "Information security standards focus on the existence of process, not its content", *Communications of the ACM*, Vol. 49 No. 8, pp. 97-100.

Theoharidou, M., Tsalis, N. and Gritzalis, D. (2013), "In cloud We trust: risk-assessment-as-a-service", in Fernández-Gago, C., Martinelli, F., Pearson, S. and Agudo, I. (Eds), *Trust Management VII*, Springer, Berlin, Heidelberg, pp. 100-110.

Tong, A., Sainsbury, P. and Craig, J. (2007), "Consolidated criteria for reporting qualitative research (COREQ): a 32-item checklist for interviews and focus groups", *International Journal for Quality in Health Care*, Vol. 19 No. 6, pp. 349-357.

Trigueros-Preciado, S., Pérez-González, D. and Solana-González, P. (2013), "Cloud computing in industrial SMEs: identification of the barriers to its adoption and effects of its application", *Electronic Markets*, Vol. 23 No. 2, pp. 105-114.

Utin, D.M., Utin, M.A. and Utin, J. (2008), "General misconceptions about information security lead to an insecure world", *Information Security Journal: A Global Perspective*, Vol. 17 No. 4, pp. 164-169.

Venters, W. and Whitley, E.A. (2012), "A critical review of cloud computing: researching desires and realities", *Journal of Information Technology*, Vol. 27 No. 3, pp. 179-197.

Wahlgren, G. and Kowalski, S. (2013), "IT security risk management model for cloud computing: a need for a new escalation approach", *International Journal of E-Entrepreneurship and Innovation*, Vol. 4 No. 4, pp. 1-19.

Wang, J. and Mu, S. (2011), "Security issues and countermeasures in cloud computing", *Proceedings of 2011 IEEE International Conference on Grey Systems and Intelligent Services, IEEE*, Nanjing, China, pp. 843-846.

Wangen, G. (2017), "Information security risk assessment: a method comparison", *Computer*, Vol. 50 No. 4, pp. 52-61.

Wangen, G., Hallstensen, C. and Snekkenes, E. (2018), "A framework for estimating information security risk assessment method completeness", *International Journal of Information Security*, Vol. 17 No. 6, pp. 681-699.

Webb, J., Ahmad, A., Maynard, S.B. 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, pp. 25-51.

Zhang, X., Wuwong, N., Li, H. and Zhang, X. (2010), "Information security risk management framework for the cloud computing environments", *2010 10th IEEE International Conference on Computer and Information Technology*, pp. 1328-1334.

Corresponding author
Ali Padyab can be contacted at: ali.padyab@his.se