International Journal of Public Administration in the Digital Age
Volume 8 • Issue 1

The Public Sector Cloud Service Procurement in Sweden:
An Exploratory Study of Use and Information Security Challenges

M. Sirajul Islam, Örebro University, Sweden*
https://orcid.org/0000-0002-7907-6037

Fredrik Karlsson, Örebro University, Sweden
https://orcid.org/0000-0002-3265-7627

ABSTRACT

This paper investigates the use of cloud services in the public sector and management of information security challenges in the procurement of such services. The findings are based on an exploratory approach that included a systematic literature review and a survey among the public agencies and municipalities in Sweden. The literature review is used to derive a conceptual framework that structures our empirical results into the three groups: 1) contractual and legal, 2) operational, and 3) managerial competency. The survey explored all these three groups. The findings show that the information security challenges are mostly related to the potential breaching of national security and laws applicable to cross-border cloud services. Most of the cloud contracts of public organizations are found to be supplier driven. In this case, lack of knowledge and awareness in managing procurement are mostly raised compared to technical risks.

KEYWORDS

Cloud Service, Outsourcing, Procurement Challenges, Procurement Management, Public Sector, Sweden

1. INTRODUCTION

Digitalization of public sector has been in progress since the 1950's (Banister & Grönlund, 2017), and innovative digital technologies continuously provoke new service models. These technologies enable citizens to access government services through multiple channels seamlessly. They also provide organizations in the public sector with the means to work together in environments which are built on complex, but scalable, interoperable infrastructures. To continue create public value, agile governance is needed (Soe & Drescher, 2018). Therefore, as the public sector worldwide tends to incorporate online service-oriented architecture across multiple domains, this has been triggering them to adopt and deal with models such as cloud computing services.

According to the ISO/IEC (2014), cloud computing is defined as an evolving paradigm "for enabling network access to a scalable and elastic pool of sharable physical or virtual resources with

DOI: 10.4018/IJPADA.302906 *Corresponding Author

self-service provisioning and administration on demand" (para. 3.2.5), whereas cloud service is described as "one or more capabilities offered via cloud computing" (para. 3.2.8). The resources referred to in this definition include, for example, servers, operating systems, networks, software, applications and storage equipment. According to Gartner (April 11, 2018) 47% of government organizations around the world are actively using cloud services. They forecast that global adoption of cloud technologies will continue to expand rapidly even in the context of COVID-19 pandemic due to the continued flexibility and agility of the innovative digital technologies. They estimate that the spending on public cloud services of the total global enterprise IT budget will exceed to 45% by 2026 from 22% in 2021 (Gartner, August 2, 2021). Furthermore, the 'Gartner's 2018 CIO Agenda' survey conducted among the CIOs in 98 countries, including 461 government CIOs, shows that technology-investments related to cloud services/solutions, business intelligence/analytics, and data-infrastructure were the most crucial in achieving organizations' missions (Gartner, January 23, 2018).

Given the society's growing dependencies on the digital environment, information security risk management in the public sector has become a major concern. Public cloud service usage is a type of outsourcing, and outsourcing is an 'evermore complex' arrangement (Gozman & Willcocks, 2015). The public sector, in general, needs to maintain some essential procedures capable of distinguishing the sensitivity of the data due to two spectrums: (1) legal requirements that public sector data should be openly available, and (2) the obligations to safeguard data that can impact national security (Gleeson & Walden, 2016). As the continuity of business is increasingly relying on the cloud computing environment, it is imperative to have carefully tailored strategic decision-making on cloud adoption. In this case, a good fit between outsourcing and business strategy is crucial for the advantages for organizational performance (Lee, 2006; Hahn et al., 2013). However, achieving such fit in these decisions is challenging, both due to practical and socio-political reasons (Khajeh-Hosseini et al., 2010). Gartner (2021) in this regard reveals that the success rate for governments' cloud deployment (63%) is a bit of behind the all-industry global average (68%). They argue that this success ratio can be improved if the government CIOs avoid cloud projects with unrealistic objectives given the realities of their organizations and focus on the agility and scalability of IT for the 'whole organization'.

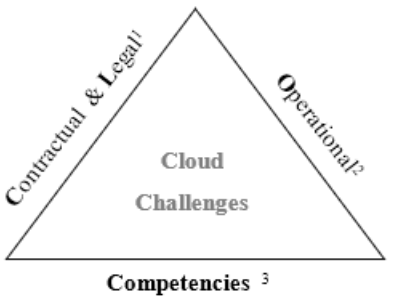
According to Zhang, Nan and Tan (2020), cloud services are transforming businesses at an ever-increasing rate on one hand and create challenges on the other due to their associated information security risks and low customization capability. Consequently, it is important to understand the information security risks related to outsourcing due to the growing information security breaching and threats on the confidentiality, integrity and availability of cloud services. However, existing studies show that we do not know much about such associated risks 'in-depth' due to the lack of research papers with well-grounded empirical evidence (Hahn, Doh, & Bunyaratavej, 2009; Benlian & Hess 2010; Ackermann et al., 2011). Muhic and Johansson's (2014) literature review on cloud sourcing in top information system conferences and journals states "[i]t is puzzling that not more research has been done on this topic which at first glance might seem researched, but on closer inspection reveals to be lacking in depth" (p. 559). Furthermore, Josep and Joan (2020) argue that research is lacking analyses that focus on IT outsourcing in the public sector, as compared with the private sector. Therefore, in light of this background, we pose the following research questions: *(1) how does the public sector use public cloud services* and *(2) what are the public sector's perceived information security challenges in the procurement of public cloud services*? We operationalize the latter of these two research questions through developing a conceptual framework to identify the groups of cloud service challenges. We present our findings in line with this framework based on a survey being conducted among the public agencies and municipalities in Sweden.

This paper is structured as follows. After the aforementioned background of the study, Section 2 reviews the related literature that leads to the development of a conceptual framework on the challenges of cloud service outsourcing. Section 3 describes the methods we have used for the literature review, conducting a survey and analysis of the data. Afterwards, Section 4 presents the findings of the surveyed data in line with the conceptual framework, followed by a discussion and conclusion in Section 5.

2. CLOUD SERVICE CHALLENGES – TOWARDS A CONCEPTUAL FRAMEWORK

There are varied types of influencing factors when using cloud services. The most common factors among them are a greater degree of administrative flexibility and intra-organizational collaboration, cost savings, and improved round-the-clock customer services. Based on the Business Risk model, Paquett et al. (2010) explore tangible and intangible information security risks related to the use of cloud computing in government. They identified risks in the areas of access, availability, infrastructure and integrity. As a result, they identify essential elements to include in any risk management plan in the public sector. Risks associated with access include unauthorized access to private data, uncertainty of the conventions and laws where the servers are hosted, and weak SLA(service-level agreement) between the agency and the vendor that may place sensitive data at risk. Uncertainty in the uninterrupted availability of services to the customers may cause severe consequences. Ceasing business operations of the vendor unceremoniously or any other unexpected outrages could be very costly, which may be due to, for example, overloads on the systems, programming errors, malicious attacks by hackers, power failure, and natural disaster. Cloud service outsourcing/procurement managers, therefore, "would need a deep understanding of the risk and impacts of even a minute's outage and acceptable levels of downtime on a site-wide basis before a contract could be awarded" (Paquett et al., 2010, p. 249). Given this, based on our literature review (see Section 3 for method details), we identify three broad challenges related to cloud service outsourcing: *contractual and legal*, *operational*, and *competencies*. These challenges are apparently integrated into each other and therefore grouped in a triangular form in Figure 1 to illustrate these intersections. Each of the challenges is briefly introduced below.

Figure 1. Three groups of cloud challenges in outsourcing



1. e.g. terms of conditions, liability, national and cross-border laws, policies, protection, privacy

2. e.g. implementation, technical, services, budgeting, vendor lock-in

3. e.g. managerial skills, know-how, vendor relationships

2.1 Contractual and Legal

A standard cloud contract, which is generally termed as an SLA, plays an important role in defining the quality and availability of services, identifying acceptable risks, allocating responsibilities, and providing enforcement mechanisms in case of the inadequacy of existing rules. However, because of the management, infrastructural, and information security complexities, contract clauses related to cloud service procurement need additional review unlike the traditional service contracts (Marston et al., 2011). According to Gartner (2017), a lack of integrity in the commitments and poorly defined SLA can impact on an organization's cloud program in several ways; it can affect the validity, quality, information security as well as the overall performance of the program. In fact, formulating a 'good contract' is challenging, because both the clients and service providers seek to incorporate their interests as far as possible. This could result in contracts that seem balanced that may potentially

overlook some realities, such as applicable cross-border laws, end-user data protection requirements, evolving technological innovations and information security threats. In regard to the potentially conflicting expectations between the service clients and cloud providers, the European Commission (EC, 2015) finds that "business and consumers still do not feel confident enough to adopt cross-border cloud services" (p. 14) and that the existing contracts often exclude, or severely limit, the contractual liability of the cloud providers.

Therefore, good outsourcing contracts are essential because of the losses that can occur due to information security breaches and mishandling of the promised services. Such contracts could protect the rights of the parties involved on fair and unbiased terms, provide accurate valuation of any losses, set clear obligations related to, for example, notifications of information security breaches, data transfers and access by law enforcement entities, creation of derivative works, and change of control (Clemons & Chen, 2011; Marston et al., 2011). From the client's perspective, Clemons and Chen (2011) suggest that a cloud contract should be designed based on three dimensions, which are performance, information security and legal recourse in resolving disputes. Gozman and Willcocks (2019) advise organizations to have a good contract which has "appropriate controls and measures for meeting regulatory obligations" (p. 245). The contractual agreements should include well-defined auditing and access rights. It means allowing organizations rights of access to the vendor's premises to assess their data management, security and architectures. According to them, "key contract provisions may consider cost and compensation, right to audit, establishing and monitoring performance standards, confidentiality and security of information, ownership and licensing, default and termination, dispute resolutions, limits on liability, insurance, customer complaints handling, and business continuity and planning as well as subcontracting" (Ibid., p. 246). To this end, Piswanger and Strick (2017) recommend using a procurement model and tender strategy as early as possible, in order to identify the challenges and object of the tender.

According to Gleeson and Walden (2016, p. 690), "there are no substantial legal barriers to the public sector adopting or procuring cloud computing". Their study on public sector cloud procurement and governance finds that, apart from practical barriers for the public sector moving to or procuring cloud services, neither national nor EU law prevents them from using cloud services. The legal aspect of the cloud service environment is related to the applicable national and cross-border laws where the data are stored and processed, access policies, protection of shared resources and intellectual property, and privacy of individual data. The access issue is mainly related to the information security policies of the organizations that outline employees' access to data and how to avoid unauthorized access (Subashini & Kavitha, 2011; Bowers et al., 2008). In a European study, Piswanger and Strick (2017) find two main categories of legal challenges in adopting cloud solutions. The first category is a general set of challenges that most organization face when moving to the cloud, such as applicable laws, how to solve disputes and deal with data protection. The second category includes challenges that are specific to the public sector and includes public procurement legislation and legal aspects about "language requirements, archiving, national defense and state secrets, fiscal and bookkeeping legislation, social and criminal procedures and health care requirements" (ibid., p. 163).

The legal implications of third-party data management represent a complex issue as there is a "potential lack of control and transparency when a third party holds the data" (Chow et al., 2009, p. 2). This is a particularly important issue in the context of the EU and Nordic region. For example, laws in the Nordic countries restrict transferring personal information to other countries, and such data can be transferred to "countries in the EU/EES, as long as a proper security level is maintained" (Norden, 2012, p. 34). Furthermore, data can be transferred to countries outside the EU/EES that meet the EU directive of Safe Harbor. Thus, the cloud service providers must meet information security standards and national laws, but the governance can be challenging because cloud computing is distributed by nature. There are still grave concerns over EU data protection laws, data location and access by the third party located in the agencies of another country. Therefore, data management is a challenging

task for public sector organizations in the EU as they need to comply with both the EU General Data Protection Regulation (GDPR) and meeting the increasing demand for self-service solutions.

2.2 Operational

Operational challenges of cloud outsourcing management are related to both the technical as well as service implementation aspects. In both cases, budgeting/financial capabilities are an important issue. Jones' (2015) case study on UK Local Authorities summarized key factors for successful cloud procurement and implementation in a number of categories. These categories are: (1) a proper way of conducting a feasibility study to identify both advantages, risks and costs; (2) commitment from senior management; (3) strong project management during implementation; (4) being able to innovate business processes that are delivered by a flexible workforce; (5) support from an in-house IT team and (6) regular arrangement of performance monitoring and evaluation.

As for the technical aspect, Zissis and Lekkas (2012) summarize information security challenges of cloud computing depending on the users as well as service levels. According to these levels, a variety of information security threats is listed. At the application level, they listed threats such as interception, data modification and deletion, and session hijacking. At the virtual level, the threats major are programming errors, software modification and interruption, distributed denial-of-service (DDoS) attack, and disrupting communication. Finally, at the physical level, they listed threats such as network attack, hardware theft, modification and interruption, misuse of infrastructure and natural disaster.

These threats could lead to serious incidents that may result in expensive service disruptions if suitable precautions are not taken properly. ENISA (2013) defines a cloud computing 'incident' as "a breach of security or a loss of integrity that has an impact on the operation of network and information system core services, which public administrations and market operators provide. The 'reportable incident' is the one that has deemed significant impact" (p. 5). The severity of impacts depends on how critical the cloud services are. Cloud services can be critical in at least two ways. First, services are used by operators of critical infrastructure to support their core operational activities. Second, the cloud services themselves support critical functionings for the well-being of citizens. A cloud incident is an evolving phenomenon that could grow with the development of new innovations that could cause new circumstances for threats. Given the contemporary context, those incidents can be categorized in five ways (Fiondella et al., 2013). These are: outage (unplanned availability of services), vulnerability (site-specific vulnerabilities of cloud providers), auto-fail (problematic automatic update of the systems that breaks core functionalities), data loss (unintended loss of data), and hacking (hacker(s) gain unauthorized access to data in the cloud service). Among these, outage and vulnerabilities are the most common and growing rapidly. Dhar (2012) therefore suggests the cloud providers should address the current challenges in a suitable way by "developing acceptable compliance and security policies, reducing the risk by developing robust infrastructure for reliability and high availability along with performance guarantee" (p.673). Abdulsalam and Hedabou (2021) further suggest that organizations should adopt 'adaptive techniques' for efficient user experience.

Identifying budget ownership and availability of adequate financial capability are important issues for operational efficiency and negotiations with cloud providers during the outsourcing process and implementation. As for budget ownership, Hahn et al. (2013) propose that benefits of the implementation of formal cloud strategy are positively proportionate to the extent of budgetary allocation by a business division for IT solutions. They state that "cloud costs are operational expenses and can be simply booked with a corporate credit card, the budget ownership influences the strategy. This could possibly turn former non-IT budgets into unwanted IT budgets where vendors will find it easy to sell directly to business divisions ('users become more self-determined […] and therefore vendors are impacted in terms of how to structure their sales')" (Ibid., p. 4).

Cloud services have the potential to offload organizations' burden of legacy systems. In this way, organization can improve their 'guardianship' either through migrating to cloud services or

modernizing their existing information systems (Pang & Tanriverdi, 2022). At the same time, Ayele and Juell-Skielse (2015) find that public agencies in the Swedish context experience increased dependency on vendors as a challenge, in particular in cases when an organization wants to deliver the service at its own premises and its own ways. Given such needs, cloud-vendors push low-cost, yet competitively value-added services. They offer attractive proposals with innovative business models to influence the "top management to think about outsourcing as a sensible low-cost alternative" (Dhar, 2012, p.665). In many cases, management may suffer from decision-making dilemmas mainly due to the potential lack of control over intellectual property, data ownership and/or overall information infrastructure. Furthermore, in the absence of a good formal contract with quality-of-service guarantees, there could be a possibility of vendor lock-in (Marston et al., 2011). The lock-in situation could be even more alarming if a client develops a unique application based on a unique platform of the vendor (Clemons and Chen, 2011). Williams and Griffin (2018) therefore call for initiating a wide range of public policies for governing cloud related services and technologies.

In fact, moving data resources towards centralized cloud systems being handled by a few suppliers could potentially pose information security problems especially in terms of endangering users' privacy and confidentiality of information. The integrated (or aggregated) framework of analysis of data in a cloud architecture streaming from various sources would "fundamentally enable the cloud supplier to know much more about its user-base than what has been voluntarily disclosed by each front-end individual user" (Filippi & McCarthy, 2012, p. 5). In order to minimize such a catch-22 situation, as described earlier, a balanced and mutually beneficial relationship between the cloud-client management and suppliers is needed. This is also echoed by Hodosi, Haider and Rusu (2020) in a study on public organizations in Sweden. According to them, cloud related risk factors can be minimized if the clients improve relationship or build mutual trust with their suppliers. In fact, as a catalyst, balancing technology-related capabilities and relationship-driven capabilities enables organizational value co-creation in the environment of emergent cloud platform ecosystem (Schreieck, Wiesche, & Krcmar, 2021). However, building up of such a relationship depends on the current capabilities of an organization to manage. Hahn et al. (2013) find that high capabilities in the governance of outsourcing through "a more formal approach for a cloud strategy" (p. 4) with more managerial independence in a decentralized organizational environment will increase the likelihood of creating flexible outsourcing relationships with the vendors.

2.3 Managerial Competencies

Competencies are organizational and managerial aspects of the cloud-challenges that inform the level of skills and proficiencies on the process and administration of cloud outsourcing. The factors that influence such corporate governance are – "organizational size, managerial autonomy and formalization attitudes" (Hahn et al., 2013, p.4). As outsourcing is a complex arrangement, an organization should adopt robust governance with a balance between the control of innovative systems' competitiveness (Gozman and Willcocks (2015). Therefore, managers in IT organizations need to be trained with the knowledge and skills necessary to develop, acquire and integrate cloud-based solutions provided by external vendors, and create and manage service level agreements with cloud computing providers.

According to Hahn et al. (2013), the size of an organization is proportionate to the degree of centralization in the coordination of IT management, i.e., smaller organizations tend to be more centralized and informal in adopting cloud strategy than larger organizations. This further indicates that centralized IT governance for cloud solutions and applications/decision-making has less managerial autonomy than the decentralized governance. Moreover, they proposed that an organization's attitude towards formalization of its policies, such as information security policies, defines the liabilities of employees. A sufficient level of knowledge about cloud providers is conducive for gaining trust. However, there is a hidden surface in this process as we do not know much about the relationship on how users and cloud suppliers "gain better knowledge (and trust) of the other party" (Venters

& Whitley, 2012, p. 193), because, on the one hand, cloud suppliers may not be sure whether they at all "cover the range of equivalence comparisons" (Ibid) as demanded in a market. On the other hand, users may face difficulties in gaining knowledge of the variety of services due to limited understanding of their 'demand for variety'. In this case, the capabilities of both the counter parties (users vs. suppliers) need to match the 'agility demanded' due to the rapidly expanding capacity of computing technologies (Ibid.).

A comprehensive survey on information security trends in the public sector conducted by Microsoft (2014) among 12,000 respondents worldwide found that the public sector also lacks coherent information security policies. According to this survey, "45% public sector cloud clients do not use standardized data classification, […] 36% do not have a plan for responding to security breaches, […and only] 24% have adequate policies and practices for secure data disposal" (Ibid., p. 1). Paquett et al. (2010) in this regard state that "a key challenge presented by cloud computing is the difficulty that exists in fully managing and controlling cloud providers outside the government. This once again illustrates the need for strong service agreements and a thorough understanding of the risks of cloud" (p. 252). Delivery, transformation and the relationship with vendors are the three outsourcing competencies that an organization needs to develop and practice (Feeny et al., 2005). To better control outsourcing implementation, such as cloud services, Plugge et al. (2016) suggest first focusing on reorganization before turning the attention to outsourcing arrangements. The first means an extended adaptation period as organization have to develop the required level of capabilities over time.

3. RESEARCH METHODS

This is an exploratory study (Venkatesh et al., 2013; Creswell & Clark, 2011) to achieve both breadth and depth in the mapping of the issues related to the information security challenges of public cloud service procurement management. This exploratory end was operationalized through a survey (Mingers, 2003) among the information systems security managers employed by the public sector in Sweden. Thus, it enabled us to explore the magnitude of the phenomena in real life settings in Sweden.

3.1 Literature Review

There are two purposes of literature review in this study – to develop a conceptual framework to systematically understand the context of the problem and to design survey questions. As for the source of relevant literature published, we did a systematic search in four data sources, such as Clarivate Analytics', Elsevier's database SCOPUS, all eight of AIS's Senior Scholars' Basket of Journals without restriction to any time period, and Google and Google Scholar that brought up some contemporary (2014-2022) documents published mainly by practitioners, which are normally not expected in academic research databases. This was done in order to minimize the risk of skipping interesting quality papers.

Several combinations of keywords were used: 'public cloud services', 'cloud service procurement', 'cloud service risk' and 'cloud service challenges'. We also used the word 'outsourcing' as a synonym for 'procurement'. Apart from the papers published in a global context, we were particularly interested in the European Union due to the context of our study. We excluded the papers based fully on a 'literature review' of other papers and considered the ones which were based on empirical studies. We found a good number of papers that covered 'public cloud'; however, there is apparently a lack of research that focuses on 'public sector cloud' computing. The search ended up with 128 publications. Finally, after careful sorting, using the inclusion criteria, 36 publications were used to develop a conceptual framework for this study. The inclusion criteria include the publications written in English and focused on cloud services in the public sector. We analyzed and thematized the sorted papers based on the guidelines suggested by Webster and Watson (2002). To thematize the review, which in the end is structured in a conceptual framework as shown in Figure 1, a concept-centric

approach was followed. The framework is generic in nature, to capture the issues being surrounded by the research question.

3.2 Survey

The questionnaires of the survey were sent out to 521 respondents using a web-based survey platform. The targeted respondents were public information security managers working at 231 public agencies and all 290 municipalities in Sweden. The overall response rate was 38% (n=199), of which 52% (n=119) was from public agencies and 28% (n= 80) from municipalities. In total, there were 32 questions with some associated sub-questions in the survey. They covered various aspects of the cloud computing (SaaS, PaaS, IaaS) environment in the public sector in Sweden, such as use, risks and incidents, experiences, procurement challenges, legal issues, vendors and contracts with vendors, centralization, and decision-making processes. The questions were a combination of closed-ended multiple choice questions and open-ended formats. In this paper, we have used only those questions that are relevant to discussing challenges with cloud services in the public sector. The survey was developed iteratively, and the quality of the questions was cross-checked (types of questions, response options and logical flow) by both the Swedish Civil Contingencies Agency (SCCA) and the Swedish Association of Local Authorities and Regions (SALAR). The analysis is guided by the structure of the conceptual framework.

4. PUBLIC-CLOUD SERVICE SECURITY MANAGEMENT IN SWEDEN

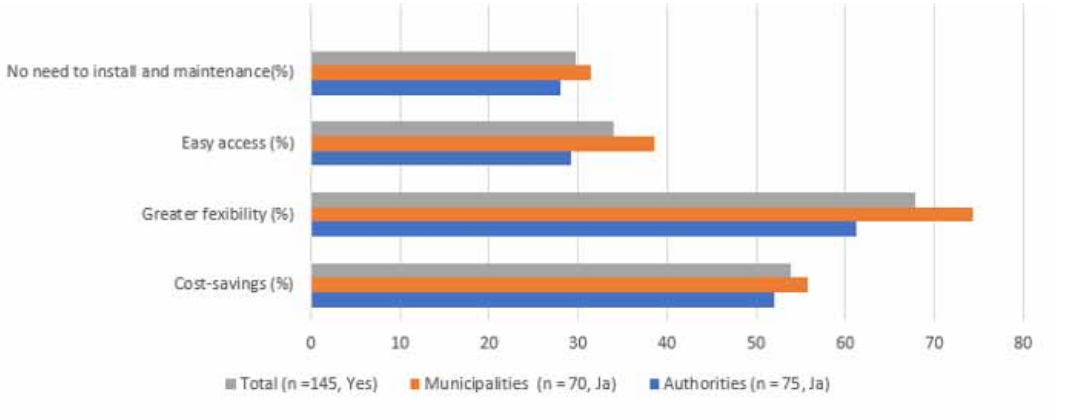
Our study is situated in the Swedish public administration context. Public administration in Sweden is structured in three levels: national, regional and local. In this study we address the national level and local levels, i.e, public agencies and municipalities. Sweden has 250 public agencies at the national level and has 290 municipalities at the local level. All public agencies and municipalities have a high degree of autonomy in how execute their tasks. Furthermore, the national level government has limited say over the local level government. Thus, joint decision-making between any of these actors are not directed by political decisions. Instead, such decisions are business agreements, based on discussions and negotiations.

With the rapid progress of networked-based transactions worldwide, security of information systems infrastructure, access to private data and ownership of intellectual properties have become a major concern. In this context and for handling other emergency-related issues at the national level, SCCA was formed in 2009. One of their tasks is to support and coordinate societal information security, including cloud computing. The Digitization Commission was set up in 2012 to develop Sweden's future roadmap for a digital society. As time has progressed, Sweden has now become one of leading countries in the EU offering digital public services and 23% of its public agencies use cloud-service related IT platforms (Pensions Myndigheten, 2016). Due to the absence of centrally administered public/government cloud solutions, Sweden largely outsources cloud services. Therefore, given the growing dependency on cloud outsourcing, the Swedish Data Protection Authority provides guidelines for the use of cloud services, especially for municipalities and cloud providers on handling personal data in line with the existing laws, such as the Data Protection Act 2018 (the supplemented version of EU's GDPR). SALAR also provides guidelines (SKL, 2017) on using cloud services in line with the requirements of the Swedish Data Protection Authority in order to avoid dubious handling of personal data.

4.1 The Use of Cloud Services by Public Agencies and Municipalities in Sweden

We asked a general question about whether the public sector organization had any contracted cloud services. Overall, 75% of the surveyed organizations, agencies as well as municipalities responded 'yes' to this question. Among them, municipalities seem to procure more contracted services (88%) than the agencies (63%).

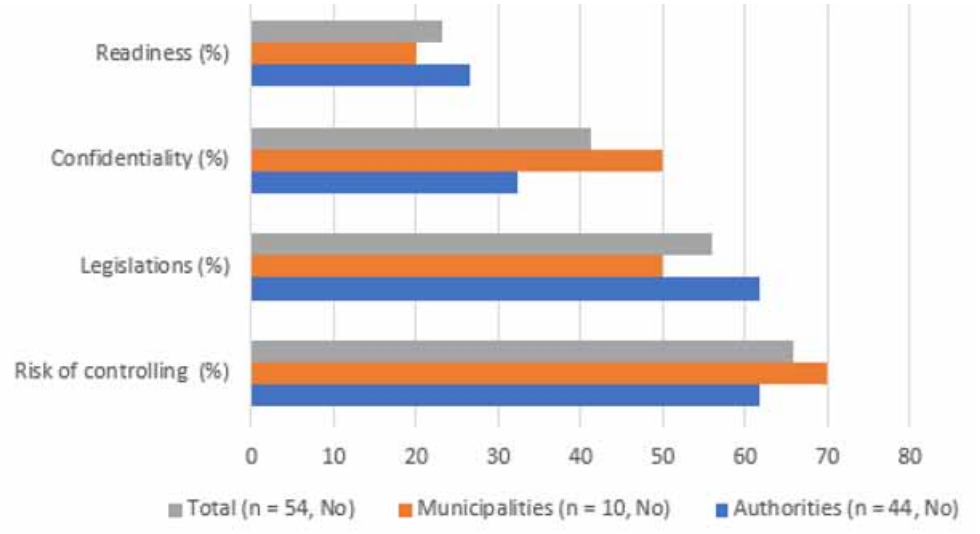
Figure 2. The main reasons for adopting cloud services



The survey found (Figure 2) that greater flexibility (68%), cost-savings (54%), easy-accessibility of specialized IT resources (34%) and no need for installation and maintenance (28%) were the four main reasons for the organizations to use cloud services. The flexibility comes in terms of handling complex IT operations, minimizing workloads and meeting on-demand capacity. With this, the organization can provide better citizen/customer services, gain operational efficiencies by focusing on the other critical tasks and minimize cost. Scalability and meeting the growing demand for the services being offered are important factors. According to an agency respondent, "*The reason why we use cloud services is because of a need to deviate from existing market products to accommodate the service-level and the kind of services we need. IT operations are more easily managed accounting-wise, receiving invoices continuously instead of high investment at certain times. Cloud services are scalable in relation to how the activity increases/decreases*".

In regard to administrative efficiency, one of the respondents from a municipality stated that the use of cloud services contributes "*increased efficiency in administrative work processes*". We found that public sector organization try to balance organizations' need for functionalities and information security. According to a municipality respondent, "*We do not pay particular attention to whether it's a cloud service or not, provided we get the requested feature. However, we usually take into account our information security requirements based on performed system security analyzes and do not outsource information if we have deemed it inappropriate*". At the same time, depending on the nature of services/activities, organizations may not have any choice, but to go for a cloud alternative. This is clearly indicated by this statement from a municipality respondent, "*For some features/services, there are no alternatives to cloud services*". One agency participant responded, "*There are some services that are difficult/impossible to get access to if not using cloud services*".

Figure 3. The main reasons for not adopting cloud services



Agencies (27%) seem to have somewhat more readiness than the municipalities (20%) to move from their current systems to the contracted clouds. However, 25% of those organizations that did not have 'contracted cloud services' in their businesses stated some major reasons. When looking at the combined results for agencies and municipalities (see total in Figure 3), these were the risk of losing control over information (66%), risk of being unable to meet current legislation (56%), risk of compromising confidential information (41%), and current organizational readiness (23%) on moving to cloud services from the existing systems. One of the agency respondents stated that due to "*a joint coordinated IT operations and to ensure a harmonized approach to information security, the use of cloud services is from the existing regulatory perspective generally not an allowed practice*". In this case, organizations seem to value more gaining greater control and mission-critical applications by running them on traditional in-house systems or on private clouds. According to an agency respondent, they had "*not procured cloud services other than virus protection as a cloud service. All other activities are on their own servers within its own premises!*".

The survey indicated that the municipalities (50%) tend to be more concerned about confidentiality than the agencies (32%). This becomes evident through a statement from a municipality respondent, "*We say in our guidelines that it is not allowed, and in the small areas where they [cloud services] are used, those cases are modules we have been forced to use them by existing suppliers. There is a big ongoing discussion with the schools, they want to use various 'classroom' services*". However, it is not always the case that organizations do not move into the procured cloud services simply for security and legal reasons. Some organizations, especially the small agencies or those which have just been formed on the basis of special legislation (e.g. a board authority with no regular staff), rely on other agencies for their IT operations and the cloud services they provide. In some cases, depending on the nature of operational activities, some organizations do not use cloud services, simply because such solutions "*have not been necessary. No need*".

We also investigated whether the respondents knew the extent to which their organizations' employees used non-procured/non-work related (e.g. Dropbox) services to solve their work tasks. In about half of the organizations (46%), such use of non-procured services existed, either to a certain or large extent. This situation was more evident in the case of municipalities (55%) as compared to the agencies (38%). Probably, the degree of decentraliation/autonomy in Swedish municipalities could explain the difference between the two types of organizations. Also, it is noteworthy that 26% of the

respondents expressed that they did not know the extent to which employees used non-procured/non-work-related cloud services. For example, one of the agency respondents in this regard stated, "*we have not conducted an internal security audit concerning the unauthorized use of cloud services*." Regarding the organizations' position on the use of non-procured/non-work related cloud services, the survey revealed that organizations largely allow their employees to do so. However, 21% (n=145) of respondents both from the agencies (28%) and municipalities (14%) mentioned that they specifically discouraged the use of non-procured/non-work-related cloud services at their workplaces.

Figure 4. Cloud service outsourcing in terms of catagories

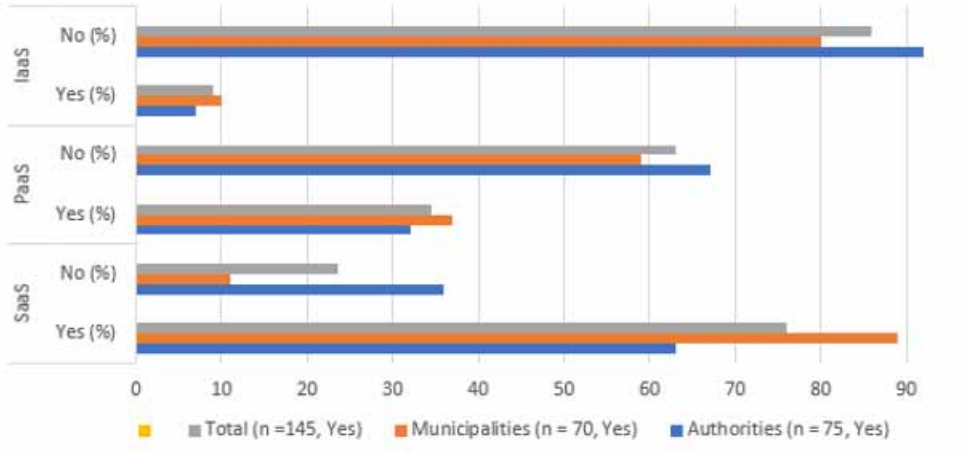


Figure 4 presents overall usage patterns for SaaS, PaaS and IaaS services being used by those organizations who which had earlier confirmed (e.g. Yes, 76%) that they had procured cloud services. As the figure shows, most organizations used SaaS (76%), followed by PaaS (35%) and IaaS (9%). SaaS was the dominant cloud-service and it was almost 26% more commonly used in the case of municipalities compared to agencies. As for the other two categories, PaaS and IaaS, the gaps were not as clear between agencies and municipalities, even though municipalities seem to take a lead role.

We used open-ended question in an attempt to capture the types of procured services in relation to SaaS, PaaS and IaaS. Understandably, due to its dominance among those three categories, the services, as they mentioned, were mostly under the category of SaaS. Furthermore, it should be noted that the findings on the types of SaaS being used were based on the 88 respondents both from the municipalities (n=51) and the agencies (n=37). Nevertheless, our empirical findings could indicate some characteristics of the types of procured cloud services. Municipalities reported the most varied types of cloud services for their educational administration and learning/pedagogical platforms as compared with the other types of applications. In the case of agencies, the applications were mostly using data sharing and storage, case and document management, education administration and learning management, customer relationship management, organizational collaboration and productivity, procurement management and feedback services.

As for the PaaS, we identified a total of 11 unique applications based on 21 respondents from municipalities and 19 respondents from the agencies. There was one particular application relating to hybrid cloud platforms being commonly found in both types of organizations. It was found that organizations used PaaS for their cloud management platforms, software development and integration, adult education, comprehensive health-care services, workflow and care management, and organization collaboration and productivity. The use of IaaS was apparently very limited. There were only three

applications that we identified based on 10 respondents for both IaaS and PaaS. The application, which was dominant in PaaS, was also commonly mentioned in IaaS.

The open-ended questions also provided an opportunity to identify the cloud service providers. In total, 29 respondents from the municipalities and 39 from the agencies provided information about procured cloud service providers. Based on this data, we identified 72 cloud service providers being assigned to provide more than 100 unique cloud services to Swedish public sector organizations, of which 76% were shared by SaaS alone. Only eight providers were commonly found in both the agencies and municipalities. In terms of number of employees, services, geographical presence, and years of operation, there was a mixture of small and big providers. Out of these providers, the top four of them are listed on PricewaterhouseCoopers's Global 100 Software Leaders.

4.2 Challenges in Cloud Procurement Management

As Table 1 shows, the legal aspect is a central challenge that covers issues, such as, how to handle cross-border national security and applicable laws in order to avoid any conflicting consequence. In fact, a typical contractual agreement should generally address those legal issues. However, as to what extent those issues are addressed, is largely dependent on the level of understanding and skills of the public service IT procurement managers. In the following, we present the major procurement challenges in line with the conceptual framework in Figure 1, i.e. contractual and legal, operational, and managerial competencies.

Table 1. What are the three main challenges in the procurement of cloud services?

Challenges (in actual numbers)	Cloud dimensions (Figure 1)	Agency (n = 119)	Municipality (n = 80)	Aggregate (n=199), Rank
To handle national security	Contractual and legal	40	31	71
To handle procurement issues	Managerial competencies	38	30	68
To handle contract issues	Contractual and legal	30	32	62
To handle supplier lock-in	Operational	29	25	54
To handle the laws applicable to cross-border cloud services	Contractual and legal	23	23	46
To handle any conflicting national laws	Contractual and legal	19	14	33
To handle cloud service comparisons	Managerial competencies	6	27	33
To handle joint procurement with other public organizations	Managerial competencies	6	13	19
To handle technical issues	Operational	12	5	17

4.3 Contractual and Legal

According to our survey, most respondents stressed the contractual and legal complexity of the procurement of cloud services. Usually, cloud contracts are supplier-driven, unless the services are mission-critical in nature. One of the respondents in this case commented "*we do not put forth any requirements in the contracts beyond what the providers offer, if there is no mission-critical cloud*

services". Table 2 shows the information security requirements that the organizations push in their contract for cloud services, in case of an absence of any readily available standardized contracts. As shown in the table, most respondents pointed out the legal requirements which are consistent with the existing national legislations relevant to information security and privacy. There are some technical and operational issues that are also deemed important for a contractual agreement, such as, clarity of responsibility and penalty in case of loss of data, requirements for data encryptions and physical security, security auditing, and continuity planning.

Table 2. Which information security requirements related to cloud services do your organization set when the cloud service provider / suppliers do not use standardized contracts?

Requirements	*Agencies (n = 75), %*	*Municipalities (n = 70), %*	*Average (n = 145), %*
Requirements for ownership of the information	63	68	66
National legal requirements	65	62	64
Requirements for clear responsibility for "data loss" (due to technical errors, data theft or infringement)	51	54	53
Data encryption requirements	47	58	52
Physical security requirements	47	58	52
Requirements for penalties if service levels are not met	45	56	50
Requirements for redundant infrastructure	43	46	44
Requirements for protection against malicious code	39	50	44
Legal requirements for the customer's handling of personal data outside the EEA	45	40	42
Continuity planning requirements	45	38	41
Requirements for opportunities for security auditing	47	32	39
Requirements for administrative staff	37	30	33
Special legal requirements for international cross-border services	22	38	30
Requirements for information security management system	49	10	30
Claims regarding intellectual property rights	22	32	27

Knowing the locations of the cloud servers and where the data are being processed is a crucial issue for any information security management. Applicable laws and regulations could be different depending on the data processing locations of the clients. According to our investigation, 34% of the surveyed public organizations always had information in their contracts that include the names of the countries where the information was processed. Significantly, it was in 'some cases' for 44% of the organizations. On the other hand, 8% of the respondents stated that the location of the data processing was not mentioned in their contracts. This was, however, more evident in case of the agencies. Notably, the remaining 13% respondents replied 'Don't know' to this question and they were mostly from the agencies.

Furthermore, in the survey's open-ended question, both the agencies and municipalities were asked about the name of those countries. Out of 114 respondents, 62% (n=71) gave responses with location information. Depending on the variety of services, organizations need to rely on several external providers and therefore their data could be processed in different locations. Instead of

mentioning exact locations of the data processing servers, 35% respondents mentioned 'somewhere in the EU/EES' for their all or specific services, while the rest stated names of the countries. Based on the location information, it was estimated that almost 95% of the cloud providers hosted their data processing servers somewhere within the EU/EES where most EU legislations concerning the single market are uniformly adopted. Notably in this case, data for 62% of all cloud services were processed in Sweden. This is to some extent beneficial in terms of dealing with uniform legislations and handling of information security and privacy related issues. Ireland (15%) had the largest share after Sweden followed by the Netherlands (8%), Norway (5%), the USA (5%), France (3%), the UK (1%) and Germany (1%). It is worth noting that the location of data-processing servers outside Sweden is almost 28% higher for agencies than for the municipalities. One of the municipality respondents, in this regard, stated, "*We usually experience less stress when services are delivered from Sweden and secondly from the EU, although in the latter case we have to a bit more thinking. We try ensure not going outside the EU*".

It was revealed that only 9% of the agencies and municipalities ensured that their contracts were regulated on the basis of international information security standards (e. g ISO 27001 and ISO 27002), while 46% replied 'sometimes'. Among those who do not base their contracts on standards, a notable 30% of the respondents were unaware of such international standards and the rest, 15%, answered 'no' to this. The cloud contractors handle sensitive data within their jurisdictions, and it is, in many cases, difficult to know how they carry out these tasks. It is therefore imperative to notify their clients in case of any security breach or malfunctioning. In this case, we found that 55% of respondents (n=145) stated that their suppliers were contractually bound to notify them about such incidents; the rest answered either 'no' or 'do not know' regarding getting notifications from their contractors. In Sweden, government agencies (but not the municipalities) are required to report to SCCA about any incident related issues. Regarding this reporting aspect, among the 75 respondents, 27% stated that contractors were liable to report directly to them and the rest were either not aware of (13%) or the contract did not include such regulation. Regarding auditing of the agreement with cloud contractors, there were varied results as 17% (n=145) said they did this on regular basis, 27% mentioned 'sometimes', while it was an equal number for 'never'. Interestingly, 29% replied that they do not know whether auditing was included in their agreements with cloud contractors.

4.3 Operational

The operational aspects we consider here are related to both the technical as well as service implementation issues with a special relationship to the information security risks. Our survey investigated the kind of experienced incidences related to cloud computing. Among the participated organizations that replied to the survey (n=145), 84% had not experienced any incidents. Those who had experienced incidents were asked to classify them according to the following options: unauthorized access to information, data loss, corruption of information and service interruption. The categories are thus related to the concepts of confidentiality, integrity, and availability (ISO, 2017). Almost all responded that the incidents were disruption of their service(s). However, it should be pointed out that the study did not investigate the causes of these interruptions.

In regard to the cloud procurement, we enquired about the extent to which the cloud service providers tailored their solutions based on the organization's information security requirements. Only 4% of the respondents replied that they had received tailor-made solutions in 'all cases' as demanded and 38% described this as 'more than half of the cases'. Notably, 24% mentioned that they did not get any customized solution during the procurement period. To this end, we also asked about the extent to which cloud service providers met the stated information security requirements in the case of incidents. Among the 145 respondents, 50% replied that they cannot answer this query as they have not had any incidents during the current contractual period and 30% responded that there had been no follow-up conducted. Only 6% said that 'everyone met the requirements', while 12% responded with

'more than half fulfilled the requirements´. The rest, 2%, revealed 'none' to 'less than half' fulfilled the information security requirements.

It is crucial to understand the types of information security risks related to the operation of cloud services as perceived by IT managers. As shown in Table 3, inadequate knowledge on managing cloud services in relation to the external cloud providers, service interruptions (especially if the service is mission-critical in nature), weak identity and data access management, data loss and security breaches, and vulnerability of system and software are the major security issues in cloud service management as identified by the managers. In regard to mission critical services, only a few critical systems are in the cloud and potential societal consequences are therefore judged by the respondents to be rather small. Furthermore, we asked whether the respondents considered it as a higher or lower risk if several public organizations use the same cloud providers. There was apparently a contradictory perception among the two groups. On the one hand, 44% respondents from both the agencies and municipalities expressed that they did not do such risk assessment. On the other hand, it was opined as 'neither high- nor low-risk' by 54% of total respondents (37% municipalities and 17% agencies). In addition, 15% of the agency respondents considered it as a 'higher risk', while it was only 1% for municipalities and many of them (17%) considered it rather a 'low risk'.

Handling the vendor lock-in is the fourth most important challenging issue apparently, both for the agencies and municipalities as shown in Table 1. Relying almost fully on the third-party vendors poses difficulties in operational activities. In this case, one of the municipality respondents mentioned that if they had their data services on their own server then they could have routines for backup. In contrast, if you buy services from external parties, it could be harder to know how to back up and restore the services if needed.

Table 3. Based on your organization's overall assessment, what are the three main information security risks when using cloud services?

Main information security risks	*Total nr of responses (n = 145, Multiple choices)*
Inadequate knowledge/awareness	64
Service interruption	59
Weak identity – reference and access management	59
Data breach	53
Data loss	46
Vulnerability in systems and / or software	40
Purposeful targeted attacks	22
Account hacking	17
Malicious software	10
Insecure APIs	10
Shared technological problems	9

4.4 Managerial Competencies

In order to off-load the burden of legacy systems and minimize cost (time, effort, resources etc.), organizations tend to seek support from external contractors. However, this has its contextual pros and cons. According to our survey, 47% of the respondents opined that it increases risk if an organization relies on the external cloud services compared to their IT operations. Therefore, it is important to have

adequate knowledge about information management and information classification in the procurement process. Understanding how to procure and what critical things to consider and assess before and after the procurements are largely dependent on managerial competences. In the open-ended part of the question, one of the managers stated, "*IT is not the problem, the problem is the managers' maturity in taking responsibility for their own information management and information security*". Above, our result shows that a good number of respondents (30%) were unaware of the need to consider international information security standards in contracts and auditing of their agreements from time to time. Many of them did not know whether they were contractually entitled to receive notifications about any security breach from their contractors. In fact, most of them perceived (see Table 3) that 'inadequate knowledge/awareness' is one of the top three main information security risks when using cloud services.

With regard to risk awareness, we asked whether the respondents' organizations performed a systematic risk analysis before and during the procurement of cloud services. Together with both the municipalities and public agencies, ranging from 'always' to 'do not know' in the questions, only 25% responded that they carried out pre-procurement risk analysis. On the other hand, 17% of the public cloud clients had always performed a systematic risk analysis on a regular basis and 60% replied that they did such assessment 'sometimes' after the procurement. In both cases – prior and during –an average of 20% revealed that they 'never' carried out any risk assessment. Among all the respondents (n=145) to this question, only 3% replied that they had no idea at all about whether they needed to carry out such risk assessment that required to hand-in their data to a third party. Prior to engaging any bilateral long-term commitment on handling sensitive data, it is crucial to check the background history of a cloud provider. In this regard, 34% responded that they always take contractors' history into consideration when procuring cloud services. Furthermore, while 36% did this task 'sometimes', 8% had never done so. Notably, 22% responded that they were not aware of doing such background checks on potential service providers.

5. DISCUSSION AND CONCLUSION

This paper seeks to answer the following two research questions: (1) how do public sector agencies use public cloud services, and (2) what are the security challenges in the procurement of public cloud services? To this end, we took an exploratory survey-approach. Thus, this paper answers the call of Josep and Joan (2020), that more research is needed on IT outsourcing, which in our case, is operationalized as public cloud services. Although our survey results are centered around the Swedish context, some lessons can still be learned in three aspects.

First, our findings show that the usage patterns between different types of cloud services differ, where SaaS is the most frequently adopted type of service by public sector organizations. This confirms earlier findings by IDG (2016) in their practitioner report. However, it might not be surprising because this is the type of cloud service that most closely relates to supporting core activities in businesses and has the most apparent potential to offer maintenance gains. Organizations need a wide variety of information systems to support their core businesses, and each of these systems also requires specialized maintenance competence. Thus, these types of information systems come with large commitments in maintenance structures, which cloud services have the potential to reduce. This might especially be true in municipalities that have a very diverse business to support.

Our results confirm existing findings (IDG, 2016) regarding the reasons why public sector agencies adopt public cloud services, thus focusing on business efficiency (Müller et al., 2015) over business effectiveness and business transformation. As is shown in Figure 2, the four main reasons for these organizations to use cloud services are related to administrative flexibility and costs. The last reason, i.e., cost, was also found in Lee at al.'s (2020) study of public clouds in South Korean government organizations. The use of public cloud services makes it possible for managers to meet demands without investing heavily in an infrastructure that needs maintenance. Public sector

organizations' focus on SaaS might, therefore, not be that surprising, because the potential cost-saving might be easily attained.

When public sector organizations consider moving to public cloud services, our findings show that it is not only based on mangers' strategic or tactical choices. Our results show that suppliers are pushing public sector organizations towards cloud services in some cases; it is the only way of gaining access to information systems that they are currently using. Jensen and Lundström (2021) have, although in a small study on the transition to cloud of two Swedish municipalities, reported a similar finding. According to them municipalities adopt cloud services for three broad reasons: competitive external environment with certain characteristics of the market and industry, availability of superior solutions, and organizational context where managers are found to be optimistic and service-centric. Given those influencing factors, they found that managers feel pressure from the cloud vendors to accept their modern solutions. Consequently, this means that managers in public organizations are at odds with achieving a good fit between outsourcing, in our case as public cloud services, and business strategy to enhance organizational performance (Lee, 2006; Hahn et al., 2013). Jensen and Lundström (2021) also point out that those 'odd fits' between several restrictions (e.g. legal), external influencing factors and exercising service-centric mindset hinder innovative abilities of the municipalities.

Second, we confirm several of the challenges related to the use of cloud services discussed by Janssen and Joha (2011), and Lacity, Khan and Yan (2016). Our findings in Table 1 show that several of these challenges are related to legal and contractual issues. Several of the challenges also relate to information security, such as national security and laws applicable to cross-border cloud services. Hildén (2021) in this regard states that Swedish public authority cannot move their services to the third-party cross-broader (e.g., non-EU, USA) vendors so readily without a proper judicial review. In this case a decentralized government model such as the one in Sweden can be a disadvantage, because there is no central authority that decides on how to implement cloud services. Instead, local managers in public organizations need to be aware of these requirements as they are free to make their own decisions about cloud services as long as they are compliant with the law. Respondents in our survey also mentioned about handling technical issues as one of the important challenges. This is in line with the findings of a study on a large Swedish local government municipality, where inflexible (i.e., limited customization) cloud-based system pose challenges for the local management for meeting the demands from a diverse range of Organizational units (Wall et al. 2021)

The more detailed analysis of the challenges related to information security risks in Table 3 shows that knowledge and awareness are raised more frequently compared to different types of technical risks. To some extent this is logical, because managers' lack of knowledge and awareness could be a primer for many of the other information security risks. If cloud services are procured without enough knowledge about and/or attention to information security, there is a risk that these services do not meet the required information security standards. In this case, it is crucial to have strong technical, methodological capabilities and relational governance not only for clients, but also for suppliers (Lacity, Khan and Yan, 2016). Cresswell et al. (2022) in this case suggest that organizations need to overcome barriers for reaping the benefits of cloud by, for examples, reducing skill gaps, improving cultural shift for external cloud hosting and initiating compatible standard and regulations. We can also see, in Figure 3, that confidentiality is one reason why the public sector does not adopt public cloud services. As for the technical information security risks, public sector organizations seem to focus most on the application and virtual levels, and less on risks on the physical level (Zissis and Lekkas, 2012).

Third, we confirm contractual challenges related to the procurement and use of public cloud services (Gartner, 2017) and relate them to information security. Both Clemons and Chen (2011) and Gozman and Willcocks (2019) have advised organizations to carefully design cloud contracts during procurement. Lacity, Khan and Yan (2016), in this case, find that clients who signed detailed contracts and used more control mechanisms with consideration of key performance indicators experienced

better sourcing outcomes compared with clients with loose contracts and fewer controls. Our results show that, in the public sector, this does not seem to be the case in practice. Instead, most of the contracts that the public sector organizations enter are supplier-driven. The only exception seems to be when the services are mission-critical.

We contribute with a characterization of the information security requirements that managers in public sector organizations push when standard contracts are not used. The importance of ownership of data and meeting existing national legislations is stressed here. Against that background, it is noteworthy that opportunities for information security auditing are pushed less frequently. The right of access to the vendor's premises to assess their data management and security and architectures is important (Gozman and Willcocks (2019), because not having such audit rights can restrict opportunities to follow up if the requirements are actually met. Thus, managers in public sector organizations need to pay more attention to this aspect of information security and include it in the contracts. Having said that, it is not enough to have these rights, managers also need to provide resources to execute audits and evaluate that their supplier deliver according to the contracts. Indeed, this is important when moving business-critical applications to the cloud.

The findings presented in this paper are comprehensive in conceptualizing the contemporary challenges in the procurement of public sector cloud services, which, we believe, could have both theoretical as well as practical significance. Due to the convenience of accessing and analyzing data, we used Sweden as a context for exploration. The Swedish context, where public agencies and municipalities have a high degree of autonomy, also means that the results are bound that this type of context. Thus, future studies could investigate countries with other degrees of autonomy in the public sector. Such studies could also examine the difference (if any) between high and low degree of autonomy in the public sector when managers procure cloud services and what type of information security challenges they experience. Furthermore, our study describes the current situation with regards to public sector's use of and information security challenges with cloud services. We provide no details about the activities executed when procuring cloud services in public agencies and municipalities, i.e., the processes that led to this situational 'snapshot'. Thus, more research is needed on these procurement processes and the decision that managers face.

FUNDING AGENCY

The Open Access Processing Fee for this article has been paid for by the Örebro University, Sweden.

REFERENCES

Abdulsalam, Y. S., & Hedabou, M. (2022). Security and Privacy in Cloud Computing: Technical Review. *Future Internet*, *14*(1), 11. doi:10.3390/fi14010011

Ackermann, T., Miede, A., Buxmann, P., & Steinmetz, R. (2011). Taxonomy of technological IT outsourcing risks: Support for risk identification and quantification. In *ECIS. 2011*. AIS.

Ayele, W. Y., & Juell-Skielse, G. (2015). User Implications for Cloud Based Public Information Systems: A Survey of Swedish Municipalities. *EGOSE '15*, 217-227 doi:10.1145/2846012.2846036

Banister, F., & Grönlund, Å. (2017). *Information Technology and Government Research: A Brief History.* Paper presented at the 50th Hawaii International Conference on System Sciences (HICSS 2017). doi:10.24251/HICSS.2017.356

Benlian, A., & Hess, T. (2010). The Risks of Sourcing Software as a Service: An Empirical Analysis of Adopters and Non-Adopters. *Proceedings of the 18th European Conference on Information Systems (ECIS).*

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009). Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control. CCSW'09, Chicago, IL.

Clemons, E. K., & Chen, Y. (2011). Making the Decision to Contract for Cloud Services: Managing the Risk of an Extreme Form of IT Outsourcing. *44th Hawaii International Conference on System Sciences (HICSS 2011)*, 1-10. doi:10.1109/HICSS.2011.292

Cresswell, K., Hernández, A.D., Williams, R., & Sheikh, A. (2022) Key Challenges and Opportunities for Cloud Technology in Health Care: Semistructured Interview Study. *JMIR Human Factor, 9*(1).

Creswell, J. W., & Clark, V. L. P. (2011). *Designing and Conducting Mixed Methods Research. SAGE Publications* (2nd ed.). SAGE Publications.

Dhar, S. (2012). From outsourcing to Cloud computing: Evolution of IT services. *Management Research Review*, *35*(8), 664–675. doi:10.1108/01409171211247677

EC. (2015). *Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions: A Digital Single Market Strategy for Europe, Report COM(2015) 192*. European Commission.

ENISA. (2013). *Cloud Security Incident Reporting: Framework for reporting about major cloud security incidents.* European Union Agency for Network and Information Security (ENISA). Retrieved from https://www.enisa.europa.eu/publications/incident-reporting-for-cloud-computing

Feeny, D., Lacity, M., & Willcocks, L. P. (2005). Taking the measure of outsourcing providers. *Sloan Management Review*, *46*(3), 41–48.

Filippi, P. D. & McCarthy, S (2012). Cloud computing: Centralization and Data sovereignty. *EJLT European Journal of Law and Technology, 3*(2).

Fiondella, L., Gokhale, S. S., & Mendiratta, V. B. (2013). Cloud Incident Data: An Empirical Analysis. *2013 IEEE International Conference on Cloud Engineering*. Retrieved from http://ieeexplore.ieee.org.db.ub.oru.se/stamp/stamp.jsp?tp=&arnumber=6529290

Gartner. (2017). *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016, Press release*. Retrieved from https://www.gartner.com/newsroom/id/3598917

Gartner. (2018). *Gartner Survey Finds Government CIOs Will Increase Spending on Cloud, Cybersecurity and Analytics in 2018*. Retrieved from https://www.gartner.com/en/newsroom/press-releases/2018-01-23-gartner-survey-finds-government-cios-will-increase-spending-on-cloud-cybersecurity-and-analytics-in-2018

Gartner. (2018). *Understanding Cloud Adoption in Government*. Gartner, Inc. Retrieved from https://www.gartner.com/smarterwithgartner/understanding-cloud-adoption-in-government/

Gartner. (2021). *Gartner Says Four Trends Are Shaping the Future of Public Cloud*. https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud

Gartner. (2021). *How Can Governments Scale Up Cloud Adoption?* Retrieved from https://www.gartner.com/smarterwithgartner/how-can-governments-scale-up-cloud-adoption

Gleeson, N., & Walden, I. (2016). Placing the state in the cloud: Issues of data governance and public procurement. *Computer Law & Security Review*, *32*(5), 683–695. doi:10.1016/j.clsr.2016.07.004

Gozman, D., & Willcocks, L. (2015). Crocodiles in the Regulatory Swamp: Navigating the Dangers of Outsourcing, SaaS and Shadow IT. *36th International conference on information systems*, 1-20.

Gozman, D., & Willcocks, L. (2019). The emerging Cloud Dilemma: Balancing innovation with cross-border privacy and outsourcing regulations. *Journal of Business Research*, *97*, 235–256. doi:10.1016/j.jbusres.2018.06.006

Hahn, C., Repschlaeger, J., Erek, K., & Zarnekow, R. (2013) An Exploratory Study on Cloud Strategies. *Proceedings of the Nineteenth Americas Conference on Information Systems (AMCIS)*.

Hahn, E. D., Doh, J., & Bunyaratavej, K. (2009). The Evolution of Risk in Information Systems Offshoring: The Impact of Home Country Risk, Firm Learning, and Competitive Dynamics. *Management Information Systems Quarterly*, *33*(3), 597–616. doi:10.2307/20650312

Hildén, J. (2021). Mitigating the risk of US surveillance for public sector services in the cloud. *Journal of Internet Regulation*, *10*(3). Advance online publication. doi:10.14763/2021.3.1578

Hodosi, G., Haider, A., & Rusu, L. (2021). Risk factors in cloud computing relationships: A study in public organizations in Sweden. *Procedia Computer Science*, *181*, 1179–1186. doi:10.1016/j.procs.2021.01.315

IDG. (2016). *IDG Enterprise Cloud Computing Survey*. International Data Group (IDG). Retrieved from https://www.idgenterprise.com/resource/research/2016-idg-enterprise-cloud-computing-survey/

ISO/IEC. (2014). Information technology – Cloud computing – overview and vocabulary. International Organization for Standardization and the International Electrotechnical Commission. Reference nr. ISO/IEC 177788, Geneva, Switzerland. Retrieved form https://www.iso.org/obp/ui/#iso:std:iso-iec:17788:ed-1:v1:en

Janssen, M., & Joha, A. (2011). Challenges for Adopting Cloud-Based Software as a Service (SaaS) in the Public Sector. *ECIS 2011 Proceedings*. Retrieved from https://aisel.aisnet.org/ecis2011/80

Jensen, L., & Lundström, L. (2021). *Navigating your way through the clouds* (Master Thesis). Department of informatics, Umeå University, Umeå, Sweden.

Jones, S. (2015). Cloud computing procurement and implementation: Lessons learnt from a United Kingdom case study. *International Journal of Information Management*, *35*(6), 712–716. doi:10.1016/j.ijinfomgt.2015.07.007

Josep, M. M.-S., & Joan, A. P.-C. (2020). IT outsourcing in the public sector: A descriptive framework from a literature review. *Journal of Global Information Technology Management*, *23*(1), 25–52. doi:10.1080/1097198X.2019.1701357

Khajeh-Hossein, A., Greenwood, D., Smith, J. W., & Sommerville, I. (2010). The Cloud Adoption Toolkit: Supporting cloud adoption decisions in the enterprise. *Software, Practice & Experience*, *42*(4), 447–465. doi:10.1002/spe.1072

Lacity, M. C., Khan, S. A., & Yan, A. (2016). Review of the Empirical Business Services Sourcing Literature: An Update and Future Directions. *Journal of Information Technology*, *31*(3), 269–328. doi:10.1057/jit.2016.2

Lee, J. N. (2006). Outsourcing alignment with business strategy and firm performance. *Communications of AIS, 17*, 2–51. Retrieved from https://www.mendeley.com/research/outsourcing-alignment-with-business-strategy-and-firmperformance/

Lee, S., Choi, Y., Ra, J., Kim, J., & Ashihara, K. (2020). Impact of public cloud computing service in Korean government organizations. *ICIC Express Letters. Part B, Applications*, *11*(3), 313–318.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing - The business perspective. *Decision Support Systems*, *51*(1), 176–189. doi:10.1016/j.dss.2010.12.006

Microsoft. (2014). *Security trends in public sector Key findings and recommendations*. Microsoft Corporation. Retrieved from https://download.microsoft.com/download/C/B/0/CB07EFE4-875A-4AD0-8FB0-90959B21E4F8/Security-Trends-in-Public-Sector.pdf

Mingers, J. (2003). The paucity of multimethod research: A review of the information systems literature. *Information Systems Journal*, *13*(3), 233–249. doi:10.1046/j.1365-2575.2003.00143.x

Muhic, M., & Johansson, B. (2014). Cloud Sourcing – Next Generation Outsourcing? *Procedia Technology*, *16*, 553–561. doi:10.1016/j.protcy.2014.10.003

Müller, S. D., Holm, S. R., & Søndergaard, J. (2015). Benefits of Cloud Computing: Literature Review in a Maturity Model Perspective. *Communications of the Association for Information Systems*, *37*(42). Advance online publication. doi:10.17705/1CAIS.03742

Norden. (2012). *Nordic Public Sector Cloud Computing – a discussion paper.* TemaNord 2011:566, Nordic Council of Ministers. Retrieved from http://norden.diva-portal.org/smash/get/diva2:701433/FULLTEXT01.pdf

Pang, M.-S., & Tanriverdi, H. (2022). Strategic roles of IT modernization and cloud migration in reducing cybersecurity risks of organizations: The case of U.S. federal government. *The Journal of Strategic Information Systems*, *31*(1), 101707. doi:10.1016/j.jsis.2022.101707

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, *27*(3), 245–253. doi:10.1016/j.giq.2010.01.002

Pensions Myndigheten. (2016). *Pensionsmyndigheten: Svenska myndigheter bör göra sig molnberedda*. Retrieved from https://www.pensionsmyndigheten.se/Molnet16.html

Piswanger, C., & Strick, L. (2017). European Innovation Procurement "Pre-Commercial-Procurement" and Cloud Computing by Reference to the Research Project "Cloud for Europe". In *4th International Conference on eDemocracy & eGovernment, ICEDEG 2017*. IEEE.

Plugge, A., Borman, M., & Janssen, M. (2016). Strategic maneuvers in outsourcing arrangements: The need for adapting capability in delivering long-term results. *Strategic Outsourcing*, *9*(2), 139–158. doi:10.1108/SO-12-2015-0031

Schreieck, M., Wiesche, M., & Krcmar, H. (2021). Capabilities for value co-creation and value capture in emergent platform ecosystems: A longitudinal case study of SAP's cloud platform. *Journal of Information Technology*, *36*(4), 365–390. doi:10.1177/02683962211023780

SKL. (2017). *Vägledning, molntjänster.* Sveriges Kommuner och Lansting. Retrieved from https://skl.se/skolakulturfritid/skolaforskola/digitaliseringskola/molntjanster

Soe, R.-M., & Drechsler, W. (2018). Agile local governments: Experimentation before implementation. *Government Information Quarterly*, *35*(2), 323–335. doi:10.1016/j.giq.2017.11.010

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11. doi:10.1016/j.jnca.2010.07.006

Venkatesh, V., Brown, S. A., & Sullivan, Y. W. (2013). Guidelines for Conducting Mixed-methods Research: An Extension and Illustration. *Journal of the Association for Information Systems*, *17*(7), 435–494. doi:10.17705/1jais.00433

Venters, W., & Whitley, E. (2012). A Critical Review of Cloud Computing: Researching Desires and Realities. *Journal of Information Technology*, *27*(3), 179–197. doi:10.1057/jit.2012.17

Wall, M. C., Goretzki, L., Hofstedt, J., Kraus, K., & Nilsson, C-J. (2021). Exploring the implications of cloud-based enterprise resource planning systems for public sector management accountants. *Financial Accounting and Management*, 1-25.

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *Management Information Systems Quarterly*, *26*(2), xiii–xxiii.

Williams, K. Y. B., & Griffin, J. A. G. (2018). Better Security and Encryption Within Cloud Computing Systems. *International Journal of Public Administration in the Digital Age*, *5*(2), 1–11. doi:10.4018/IJPADA.2018040101

Zhang, Z., Nan, G., & Tan, Y. (2020). Cloud Services vs. On-Premises Software: Competition Under Security Risk and Product Customization. *Information Systems Research*, *31*(3), 848–864.

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. doi:10.1016/j.future.2010.12.006

M. Sirajul Islam (Siraj) is an Associate professor in Information Systems at the Informatics Department of Örebro University School of Business, Sweden. Siraj is specialized in teaching and research in the areas of digitalization at the individual, societal and organizational levels, eGovernment, Management Information Systems, ICTs for rural development (ICT4D), Design Science and Qualitative methods in IS research. He has more than 20 years of experience as a faculty member as well as researcher in Sweden, France, the Czech Republic, Bangladesh and Rwanda. Siraj is at present the Director of Master's Programme in Infor-mation Systems (Information Security Management) and leading a research team called 'ICT for Crisis Management (ICT4CM)' within the Centre for empirical research on information systems (CERIS) at the Örebro University. He has been actively involved as an Editor of some reputed journals related to information systems namely Electronic Journal of Information Systems (EJISDC), Information Technology for Development (ITD), and Journal of Global Information Technology Management (JGITM).

Fredrik Karlsson is professor in Informatics at Örebro University, Sweden. He received his PhD in Information Systems Development from Linköping University. His research on information security, tailoring of systems development methods, system development methods as reusable assets, CAME-tools, requirements engineering, method rationale and electronic government has appeared in a variety of information systems journals and conferences. Some examples are European Journal of Information Systems, Journal of the Association for Information Systems, Computers & Security, Strategic Journal of Information Systems, and Scandinavian Journal of Information Systems.