Cloud Inspector: A Tool-Based Approach for Public Administrations to Establish Information Security Processes Towards Public Clouds

Michael Diener[1] and Thomas Bolz[2]
[1] *University of Regensburg, Regensburg, Germany*
[2] *IU International University of Applied Sciences, Erfurt, Germany*

Keywords: Cloud Computing, Public Administration, Information Security Management, Security Audits.

Abstract: Digitization is on the rise in Europe's public administrations. Since the Covid-19 pandemic began, public cloud services have become essential in this domain. However, there are still security concerns about the usage of external cloud resources in business processes of public authorities, although numerous technical concepts for improving security are already available. In this paper, we focus on internal processes of information security management systems (ISMS) in public administrations. We identified potential challenges such as a lack of knowledge about cloud security and unclear roles and responsibilities when using ISMS tools in this application domain. As a possible solution, we present a tool-based approach that is based on an easy-to-use online questionnaire, which can be automatically evaluated based on predefined sentiments. With this approach, we can provide the required visibility into the status quo of public cloud security while integrating various stakeholders within public administrations into a holistic ISMS process.

1 INTRODUCTION

Cloud computing opens the possibility for organizations to access services from a pool of theoretically infinite IT resources without the need for massive up-front investments in data centers and infrastructure (Mell et al., 2011). The public cloud (i.e., Amazon Web Services, Google Workspace, Microsoft 365, etc.) is one of the proposed deployment models and is becoming more and more widely adopted. Gartner forecasts cloud computing to reach nearly $600 billion in revenue by 2023 (Gartner, 2022). In general, cloud computing offers two significant advantages to organizations: cost savings and flexibility for business processes (Armbrust et al., 2009).

Although cloud solutions have been on the market for more than 10 years, this software model is only now being increasingly implemented in public administrations (Al-Shargabi et al., 2020). The reasons for these developments are manifold. During the Covid-19 pandemic, cloud services made it possible for government agencies to quickly and easily provide tools to solve practical problems. Such as collaboration platforms and online calendars citizens could schedule their vaccinations (Tambou and Pato, 2021).

Despite recent developments regarding cloud computing in public administrations, the maturity of digitization in European countries is still uneven (EU Commission, 2022). The Digital Economy and Society Index 2022 shows that Romania, Greece, Bulgaria and Slovakia have the lowest scores in digital public services within the European Union.

Nevertheless, the scope of digital public services will sooner or later increase in all European countries. Regulation (EU) 2018/1724 enforces single digital gateways in European public authorities to enable citizens to access government services (European Union, 2018). Consequently, public administrations in Europe will also have to invest in innovative cloud services, as not all of them have the capabilities themselves to provide their own IT resources to meet legal requirements.

However, cloud computing in public administrations also faces numerous security and privacy issues, leading to enormous challenges as resources in public clouds are accessible via the Internet (Armbrust et al., 2009). In recent years, cyberattacks against public administrations have increased dramatically (KonBriefing Research, 2022). If sensitive or personal data is processed in cloud infrastructures, well-established information security processes must meet the basic protection goals of confidentiality, integrity and availability (Markus and Meuche, 2022; Samonas and Coss, 2014).

Diener, M. and Bolz, T.
Cloud Inspector: A Tool-Based Approach for Public Administrations to Establish Information Security Processes Towards Public Clouds.
DOI: 10.5220/0011694900003405
In *Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023)*, pages 543-551
ISBN: 978-989-758-624-8; ISSN: 2184-4356

For the reasons mentioned above, public administrations are in a dilemma. On one hand, they have to rely on outsourcing strategies such as cloud computing to remain fit for the future. On the other hand, there are still major concerns about the security of data in clouds. In addition, established approaches such as FedRAMP[1] are unsuitable because they are not adaptable within European public authorities due to security concerns. European cloud projects such as Gaia-X[2] are still in an early stage of development and do not currently offer practical solutions for public authorities. Cloud certifications, which are based on established standards like the ISO 27000 family or the German C5 standard, are mainly helpful during the procurement phase of cloud services (Wang and Bashir, 2022). Their validity becomes obsolete over time and cloud customers must conduct regular internal audits of cloud services or Cloud Service Providers (CSP) anyway. Furthermore, there are many tools available on the market that can provide support to organizations in implementing information security management processes in the context of cloud computing, but some issues are still unresolved in our view, which we have identified in our practical research work. Therefore, an appropriate approach for public authorities is needed so that public clouds can be integrated securely in business processes.

Based on this practice-inspired problem, we started our research process that follows the principles of the Action Design Research (ADR) methodology. Together with the Chief Information Security Officer (CISO) and practitioners from departments of a public administration, we researched and developed an innovative artifact that tries to solve the described problem. To the best of our knowledge, this work is the first research paper that examines the application of a tool-based approach, including an interactive questionnaire, for managing information security of public clouds in the field of public administrations.

The remainder of this paper is organized as follows: After examining related work on information security management due to cloud computing within public administrations (Section 2), we explain the ADR methodology that guided the conceptual design process (Section 3). Section 4 describes the conceptual design and requirements for a tool-based method. Based on this we explain in Section 5 the development of our prototype, which we named Cloud Inspector. Next, we evaluate the improvements in terms of information security processes of a public administration for managing public clouds (Section 6). The last section concludes the paper and gives an outlook.

2 RELATED WORK

2.1 Tool-Based Information Security Management for Public Clouds

Although certifications of cloud services are supposed to ensure security and other aspects of CSPs, they no longer represent the actual status quo of a cloud. In their research, Lins et al. investigate the requirements for the application of continuous monitoring of cloud services (Lins et al., 2019). This is understood to be an ongoing process to monitor the implemented systems and applications of a cloud service and to detect deviations accordingly. Based on predefined metrics, which must be provided by CSPs, the evaluation is carried out with the support of tool-based monitoring systems, making it possible to carry out continuous and dynamic cloud certification. However, this assumes that the metrics provided by the CSP are transparent, complete, and trustworthy.

In contrast to this approach, external audits of cloud services are often still carried out with classic software applications (e.g., Verinice, Eramba, etc.) to evaluate security processes based on predefined controls (Antunes et al., 2022). This makes it possible to derive potential IT risks and coordinate the management of security measures to improve the IT security of cloud services. Recent approaches in research pursue the automation of information security risk management processes (Sterbak et al., 2021).

In addition, specific cloud evaluation solutions were developed by researchers to offer the possibility to check the compatibility of Software as a Service (SaaS) solutions in accordance with service level agreements. For example, the tool Clouditor allows predefined checks to be performed against various public clouds such as Microsoft Azure (Stephanow and Banse, 2017). In their research, Diener et al. presented an AI-based tool to support the selection of appropriate cloud services depending on the sensitivity of data (Diener et al., 2016). Furthermore, numerous self-assessment tools have been designed and researched, which give IT managers the possibility to evaluate their cloud services with the help of concrete questionnaires. For example, Cidres et al. have developed a self-assessment tool that can support public administrations in Portugal in the selection of CSPs (Cidres et al., 2020).

2.2 Information Security Management in Public Administrations

Szczepaniuk et al. conducted an empirical study between 2016 and 2019 to explore the nature of the

[1] https://fedramp.gov

[2] https://gaia-x.eu

implementation of information security management systems in public administrations in Poland (Szczepaniuk et al., 2020). As part of their work, they found that the prevalence of information security management systems correlates strongly with legal requirements. Particularly the introduction of GDPR regulation and the NIS Directive. The authors of the study recommend the implementation of several different procedures and models to increase information security in public administrations. Chodakowska et al. conducted a comprehensive online survey with Polish municipalities and cities regarding the implementation of security policies (Choodakowska et al., 2022). The evaluation revealed that there is indeed a lack of practical implementation of cybersecurity rules, which increases the risk of cyberattacks.

Another study was conducted by Rehbohm et al. in which several CISOs in Germany were interviewed about the management of information security in governmental organizations (Rehbohm et al., 2019). The study results show that there is a great need for research in this field to prepare authorities and governmental institutions for the requirements of cyber security.

In addition, Moses et al. surveyed several German municipalities regarding the implementation of information security management (Moses et al., 2022). The results show that the documentation processes are a major challenge, especially for small local governments. In addition, there is a lack of appropriate tools to drive the development and establishment of information security management systems.

3 RESEARCH METHODOLOGY

For our research, we use the ADR method (Sein et al., 2011), which is widely established as a research approach for finding solutions to practical problems. ADR relies on close collaboration between researchers and practitioners. It provides a framework for dynamic collaboration between the two parties and defines four main stages with several principles.

Stage 1 focuses on the **problem formulation**, initiated by researchers, practitioners or end-users. Initially, it is necessary to establish an ADR team consisting of practitioners, experts and researchers. An important aspect of this stage is that the definition of the problem is made as an instance of a class of problems. Consequently, the range of theories available in research increases. Another principle in this stage requires the development of an artifact that considers existing theories.

In the following, stage 2 addresses activities in **building, intervention, and evaluation** (BIE). In this stage the reciprocal shaping of the artifact in an iterative process is conducted. In general, the members of the ADR team are heavily involved in the design process as they continuously evaluate the emerging artifact. It is therefore important that ADR teams are made up of members that import different perspectives and expertise to the design process. In our research project, the ADR team consists of researchers from business information systems and cloud security, as well as of CISOs and business users from a public administration.

While working on stages 1 and 2, the researchers simultaneously carry out the **reflection and learning** stage. This ensures that the knowledge can be continuously transferred to a broader class of problems. Consequently, the artifact developed in this research work does not only improve the establishment of security processes with respect to the usage of public clouds in public administration, but also implementations (i.e., IoT-devices in the context of smart city projects) within the overall information security management process.

Finally, the last stage **formalization of learning** presents the results of the research, generated during the development of the procedure and its adaptation to the organizational context. In order to fulfill the ADR principle generalized outcome, the knowledge of the resulting artifacts was abstracted.

4 CONCEPTUAL DESIGN OF THE TOOL-BASED APPROACH

By applying the ADR method, we first start formulating the problem with the help of observations and subsequent workshops with experts. Based on the identified research questions, we perform stage 2 by iterative cycles.

4.1 Problem Formulation

4.1.1 Findings in Security Management Processes

We started our research in November 2021. One of the authors of this paper is CISO at a city government with more than 4,000 employees using more than 800 different application processes. In his role as CISO, he is responsible for information security management and has a solid overview of ongoing IT projects. In parallel to his work, he is conducting research on cloud security.

The trigger of our research was a series of requests from various offices of the city government regarding the adoption of external cloud services for different concerns. For example, the foreigners department needed a cloud-based video conferencing solution that would allow external translators to be involved in conversations with foreign citizens. Already during COVID-19 pandemic, a cloud-based web application was needed by the city government's population protection department to support appointment management for vaccinations.

An even bigger challenge was the investigation of a minor IT security incident in a public cloud used for collaboration by more than 40 administered schools. Specifically, the public cloud offers a SaaS application that facilitates communication between school administrators, parents, and students. The reason was that it was not defined which administrative tasks the schools had to perform on their own responsibility. Therefore, a regular update of the user management in the SaaS application was not carried out for, which led to the effect that users had access they should no longer have.

All these use cases of public clouds in public administration had in common that they did not start as a traditional IT project, but more or less on demand. In many cases, it was not clear which entity would assume responsibility for a cloud that had already been procured, or later for a planned cloud solution. Thus, it was initially difficult to identify the responsible officials in each case and to integrate them into the cloud security audit process. Even more challenging was the actual execution of the cloud security audit using an existing ISMS tool that manages all IT assets of this public administration.

During the problem formulation stage, we also determined the composition of our ADR team. In addition to the researchers, practitioners from the public administration from different areas are also integrated, e.g., Chief Information Officer (CIO), E-Government Manager, In-house Software Developer, Data Protection Officer (DPO), IT-Project Controllers and the five people from the previous expert interviews. The latter will be considered as Cloud Product Owners (CPO), each responsible for the IT security of the adopted cloud. All members of the ADR team will be intensively involved in the evaluation of the emerging artifact in the BIE stage.

4.1.2 Research Questions

Inspired by the practical issues and a continuous review of prior research work on this topic, we identified the following research questions (cf. table 1) to address a broader class of problems in our studies.

Table 1: Research questions.

RQ 1	What needs to be changed in public administrations in order to keep CISOs up to date regarding the security state of adopted public cloud solutions?
RQ 2	How can cloud managers in public administration organizations be better integrated into the information security management processes?
RQ 3	What enhancements do ISMS tools need to support non-experts in performing systematic and regular security audits of public clouds?

4.2 Building, Intervention and Evaluation

Between March and June 2022, we reciprocally shaped the basic design of our tool-based method. Our interdisciplinary ADR team was strongly involved in this process, so that ideas of various roles and stakeholders could be integrated into the ongoing development process. We also forced a continuous abstraction and reflection of the generated knowledge from practice towards the state of the art of research.

During this time, we created a tool-based method for public administrations, so that responsible parties are enabled to improve the security of public clouds as part of a guided ISMS process. To achieve this goal, we conducted two workshops with the ADR team. In addition, we have temporarily drawn on the knowledge of other experts, including three external CISOs and two certified ISO 27001 auditors.

The first workshop focuses on the question of how tool support in public administrations can be improved to enhance the integration within ISMS processes in context of public clouds. Specifically, the results should identify features that can be used during the intended prototype development. On this basis, a design prototype was then developed in the second workshop with the focus on making it as easy as possible for end users in public administrations (i.e., cloud product owners in different departments) to carry out regular and systematic security audits of public clouds.

4.2.1 Workshop 1: Requirements for Enhanced Tool-Support

In the first workshop, the ADR team dealt with functional requirements that are decisive for the development of the prototype. The central question was which enhancements and optimizations are required so that cloud security audits can be carried out more successfully with the support of our tool?

To identify requirements that are as relevant to practice as possible, we simulated the performance of a cloud security audit. For this purpose, we created a simple questionnaire in our existing ISMS tool and attempted to work through it with members of the ADR team. Moreover, we observed together in the workshop how the use of the ISMS tool by individual team members has been perceived. In parallel, interesting observations or showstoppers were documented. We have repeated the same process again with an open-source ISMS tool, which is very similar in structure and functionality to the first one. Subsequently, we discussed the observations identified with the stakeholders.

In general, we were able to identify several shortcomings in both tools considered. Employees who have limited IT knowledge and who obtain the role as a CPO need a comprehensive instruction in the use of an ISMS tool. In addition, ADR members agreed that using an ISMS tool can become difficult after a long period of non-use.

It was noticeable in both tools that the application of questionnaires for known standards (e.g., ISO 27001, ISO 27017, etc.) proved difficult. Although available templates for security requirements (e.g., sample questionnaires, check controls, etc.) can be imported into the tools, the questions always refer one-to-one to the entire requirement. If several different requirements are described in a security requirement, the required granularity cannot be mapped with classic questionnaires. However, this problem does not only appear in the public administration sector.

Another problem was that the answers given by CPOs to security requirements had to be reviewed in detail by CISOs after the cloud audit was completed. In all tools, it is necessary for CISOs to identify insufficient answers to derive appropriate suggestions for security measures. By default, multiple choice answers can be filtered, but it is not possible to distinguish between good and bad answers. For example, the value yes in one answer can be interpreted positively, while in a completely different scenario it must be considered critical.

Taking all aspects into consideration, we were able to derive five major requirements that are relevant for a tool-based approach:

- **Accountability.** CPOs need to be aware of their responsibilities in terms of organizational security requirements for the services they are assigned from public clouds.
- **Duration.** Since audits of information security processes represent an additional time commitment for CPOs, short and precise routines must be developed to achieve high acceptance rates.
- **Self-Explaining Approaches.** Efficiency also plays an important role in conducting various cloud security audits as these must be well organized and understandable for CPOs, applying basic principles.
- **Simplicity.** The evaluation of answers from the questionnaire on specific security requirements must be quick and precise. This means that descriptive statements about the status of security requirements must be avoided. This is necessary from the point of view of CPOs and CISOs because regular and recurring security audits require an enormous amount of time.
- **Automation.** It must be possible to process and evaluate the CPOs' responses automatically. On the one hand, this should prevent time-consuming revisions. The time saved can be used for more important topics in information security. On the other hand, it can also reduce errors regarding the interpretation of statements from the CPOs, since the mindless evaluation of recurring facts is no longer necessary.

4.2.2 Workshop 2: Graphical User Interface of the Prototype

Based on the knowledge gained so far during the BIE stage, the ADR team elaborates the graphical user interface of the prototype in the following workshop. We have come to the conclusion that for security audits of public clouds, the traditional ISMS tools must be used, but with an improved self-explaining and easy-to-use concept of the web-based questionnaire. This part of an ISMS tool must include the developed requirements (cf. workshop 1) so that the identified shortcomings can be eliminated.

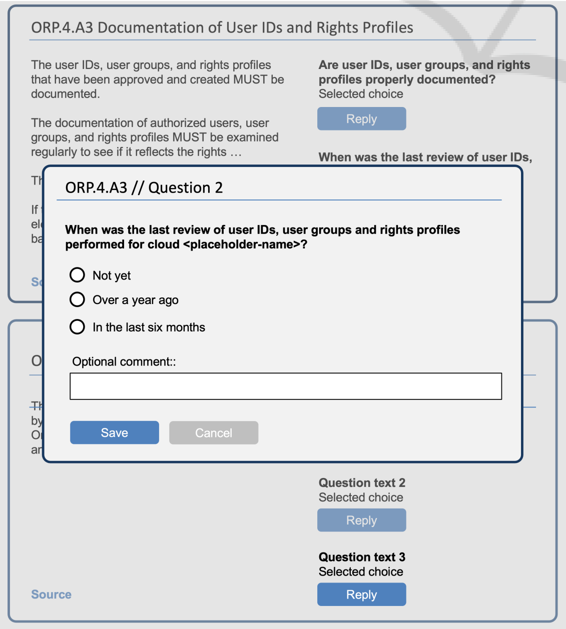
In several cycles within this workshop we have advanced the development of the prototype graphical user interface by considering existing research work (cf. stage 3: reflection and learning). Essentially, three central design principles have inspired our thinking:

1. **Central Asset Repository.** All data relating to information security management processes need to be stored in a central database (Müller et al., 2011). In our case that means, that public cloud data must be assignable to one or more organizational units of a public administration. In addition, the states of the respective security requirements need to be documented for each of these relations.
2. **Web-Based Questionnaire.** These questionnaires are easily accessible for all stakeholders

and the processing of online-supported dialogues is a very simple and quick way to collect the required data on existing conditions in a structured manner (Taniguchi et al., 2018). In relation to our problem situation, we can use computer assisted web interviews (CAWI) to obtain the necessary answers to questions about concrete security requirements. In our prototype, it should be possible to map relations as follows: Standard → Requirement → Question → Answer option. In addition, we have considered using placeholders in questions so that CPOs can keep track of what they are always providing information about when editing the questionnaires. This meets the demands for simplicity.

3. **Sentiment Analysis.** To carry out a computer-aided evaluation of the security level of a public cloud, we will apply the principles of sentiment analysis (Feldman, 2013). Using predefined classes of sentiments (e.g., positive, neutral, negative, etc.), it is possible to derive an attitude about the existing level for a concrete security requirement. For example, a response is considered negative if there is a lack of current IT documentation for an application. In this respect we have created the prerequisites for automated verifications of the given answers.

Ultimately, the considerations were incorporated into the design of the user interface of the web-based questionnaire (cf. figure 1).



ORP.4.A3 Documentation of User IDs and Rights Profiles

The user IDs, user groups, and rights profiles that have been approved and created MUST be documented.

The documentation of authorized users, user groups, and rights profiles MUST be examined regularly to see if it reflects the rights …

Are user IDs, user groups, and rights profiles properly documented?
Selected choice

When was the last review of user IDs,

ORP.4.A3 // Question 2

When was the last review of user IDs, user groups and rights profiles performed for cloud <placeholder-name>?

○ Not yet
○ Over a year ago
○ In the last six months

Optional comment::

Question text 2
Selected choice

Question text 3
Selected choice

Figure 1: Proposed design for questionnaire.

The picture shows two security requirements of BSI IT-Grundschutz-Compendium. This standard was assigned for the audit of a public cloud. The first security requirement refers to the control *ORP.4.A3 Documentation of User IDs and Rights Profiles*, the second to the following control *ORP.4.A4 Distribution of Tasks and Separation of Roles*. The interviewed CPO can thus easily keep track of the reviewed security requirements. The security requirements are delimited from each other by graphical frames. In the left part of the frame, the detailed information on the security requirement is presented in a structured manner. In the right part, the individual questions are listed. These can be answered by clicking on the button "Reply". After a click, a modal dialog opens in which the predefined answer options of the selected question are displayed.

5 PROTOTYPE DEVELOPMENT

Based on the elaborated results, in the following we describe the structure and functionality of the developed prototype. For this purpose, we first look at the backend of Cloud Inspector, then at the end-user frontend that is used by CPOs. Finally, we outline how our tool was implemented in the actual approach within our public administration. We designed the prototype by utilizing the programming frameworks laravel[3] and livewire[4]. Apache is used as web server while data is stored in a MySQL database. The prototype was developed between May and July 2022.

5.1 Question Management

In this sub-section we describe the backend of our prototype. It is also used to launch security audits of public clouds. A relationship is established between the public cloud (asset), the CPO (auditor) and the security requirements (audit template). Through this assignment, auditors automatically receive an email with the link to the online questionnaire.

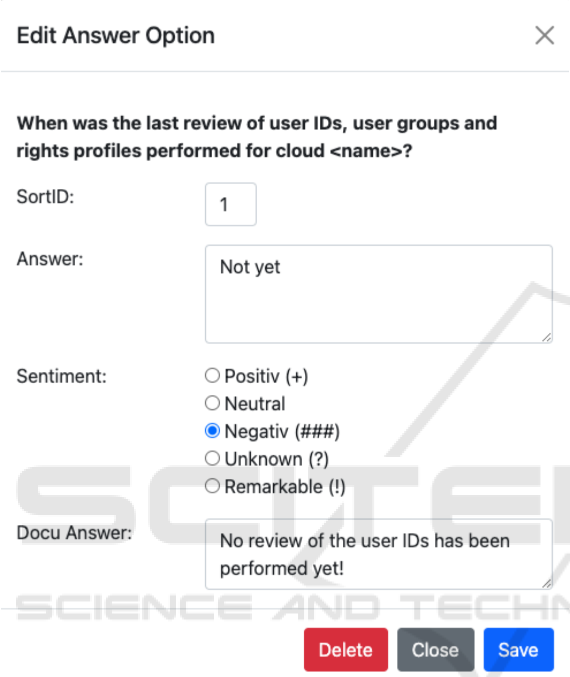
In the following, we will look at the management of questions (cf. figure 2). A question essentially consists of the question text, the definition of an answer type and the assignment to a security requirement. A security requirement can comprise of several questions. A question can include several answer options if a checkbox or radio button has been selected as the answer type. Placeholders can be integrated in the question text in order to display dynamic identifiers such as the name of the public cloud in the online

[3] https://laravel.com

[4] https://laravel-livewire.com

questionnaire.

In figure 2, the dialog for an answer options is displayed in the foreground. For each answer option, an individual sentiment can be predefined. In this respect, a one-time definition of the sentiment for a given response option already takes place before security audits are performed. Consequently, highly automated evaluations of the questionnaires can be carried out to the greatest possible extent. This saves a great deal of time and avoids interpretation errors.



Edit Answer Option

When was the last review of user IDs, user groups and rights profiles performed for cloud <name>?

SortID: 1

Answer: Not yet

Sentiment:
○ Positiv (+)
○ Neutral
● Negativ (###)
○ Unknown (?)
○ Remarkable (!)

Docu Answer: No review of the user IDs has been performed yet!

Figure 2: Sentiment specification of an answer option.

5.2 Frontend of Cloud Inspector

In this subsection we explain the user frontend of Cloud Inspector which is used by CPOs to answer questions about security requirements due to the status quo of public clouds. As a result of the creation of a new security audit, CPOs receive an email that is automatically sent by Cloud Inspector. This email contains a comprehensive explanation of why the auditor is receiving this email and what activities need to be done next. This approach avoids unnecessary queries regarding the facts and the operation of the questionnaire.

This email contains a link that leads to an overview in the frontend in which the assigned security audits are displayed. The main interface was deliberately designed to be simple so that CPOs can quickly find their way around. The central overview clearly shows the progress made in answering the questionnaire for each public cloud security audit.

During the development phases, we repeatedly had direct contact with members of the ADR team and presented and discussed the status of the frontend. In this respect, we lived up to the principle of an authentic and concurrent evaluation of our results. Based on these interactions, we were able to make a few significant improvements to Cloud Inspector.

One essential change was the replacement of the login form with a single sign-on concept that integrates a secure Kerberos authentication. This allowed us to lower the barriers to entry, getting CPOs to complete the questionnaires. In addition, we have improved the online questionnaire so that the answers entered by CPOs do not have to be answered all at once. This had the advantage for CPOs that they could work on individual questions successively without having to worry about losing the data already collected.

6 EVALUATION

Between July and August 2022, we reviewed the proposed tool-based approach. Our goal was to determine to what extent we could achieve improvements in our public administration by implementing Cloud Inspector as part of our information security processes. For this purpose we tested the applicability and acceptance of Cloud Inspector in our public administration with several CPOs. In this context, we have conducted security audits for several adopted public clouds by applying the developed tool-based approach.

6.1 Use Case

A typical use case for performing a security audit is checking the validity of user identities within an application or computer system (Osliak et al., 2021). Since we apply the German BSI standard as ISMS framework in our public administration, we have selected the module *ORP.4 Identity and Access Management* from the compendium (BSI, 2021) to perform this security audit.

The objective of this module is to validate that only those user IDs have access to a cloud system for which they are authorized. Access for a user who is no longer authorized must be revoked promptly. To ensure this objective is achieved, regular security audits must be performed to detect user identities that are no longer authorized. The department that uses the application must decide whether a user is authorized or not.

For the evaluation of our tool-based approach, we applied the basic requirement *ORP.4.A3 Documentation of User IDs and Rights Profiles* to verify the validity of user identities in adopted public clouds. The BSI requirement ORP.4.A3 includes several sub-requirements. Using the Cloud Inspector's question manager, the CISO was able to create multiple sub-questions at a fine granular level. By using placeholders in the question texts, it was possible to generate individual question texts for each unique public cloud. During the evaluation, we observed that this feature significantly improved comprehensibility among the CPOs.

With respect to the basic requirement ORP.4.A3, we derived 4 detailed questions. All questions consisted of multiple choice answers, each defined with a specific sentiment value. We asked 2 CISOs to model this issue in the question manager of Cloud Inspector. On average, this activity took no longer than 10 minutes. Under real conditions, we modeled 3 public cloud assets in the repository. Based on this, each CISO had to start a security audit on each public cloud asset with the baseline requirement ORP.4.A3. In sum, this activity could be completed in less than 1 minute.

During the period of the security audit, we received feedback from the CPOs that they were able to open the Cloud Inspector front end without any problems and start working on the assigned questionnaires. No further explanation of how our tool-based method works was required. Because we had informed the participating CPOs about our laboratory experiment, all respondents completed the questionnaires within one working day. Compared to the situation prior to our research project, applying our developed tool-based approach enhances the collaboration between CISO, DPO and CPO in a simple and self-explanatory manner.

6.2 Formalization of Learning

Overall, our work has enabled us to identify three aspects that are relevant for functioning ISMS processes in public administrations in the context of cloud security auditing.

- **Regulations.** Clear regulations are needed with regard to roles and responsibilities in connection with the procurement, implementation and the use of public cloud services.
- **Awareness.** Employees of a public administration need to have a basic understanding of cloud computing and information security. This is the only way to identify deviations in the security process at an early stage by all parties involved.
- **Tool Support.** ISMS processes must be simple, transparent and automatable in order to achieve a high acceptance rate among the involved stakeholders. Public clouds must be regularly audited for security, which means that data must be regularly collected using established organizational processes.

7 CONCLUSION AND FUTURE WORK

In this research paper, we have addressed the problem of implementing security audits of public clouds in the holistic information security management process within public administrations. To address this practical problem, we chose to apply the Action Design Research method. Based on the derived research questions, we have been able to address several scientific aspects of the identified practical problem.

Our work provides several research contributions. We clearly identified various classes of problems that occur in public administrations. In interdisciplinary workshops, we identified technical requirements for managing security of public clouds in public administrations. The main contribution of this research work deals with the optimization of information security processes for more efficient conduction of cloud security audits within public administrations. For this purpose, we developed a tool-based method based on a web-based questionnaire with predefined answer options tagged with a sentiment. We have developed and evaluated Cloud Inspector, which can meet these requirements in public administrations. We evaluated the developed Cloud Inspector against the defined practical requirements and found that this approach opens a way for public administrations to use public clouds more securely. In general, our approach could help public administrations to implement a secure digitization strategy based on public cloud services.

With respect to our tool-based method, we have identified several issues that should be investigated in future research. One is to develop a technique to help public administrations keeping track of the security state of adopted public clouds. Secondly, a concept for the simple and rapid implementation of security processes in public administrations needs to be developed to avoid unnecessary loss of time in the realization of urgent security measures. In addition, we found a lack of literature regarding concepts of raising awareness of employees in public administrations in the secure handling of cloud services.

REFERENCES

Al-Shargabi, B., Al-Jawarneh, S., and Hayajneh, S. (2020). A cloudlet based security and trust model for e-government web services. *Journal of Theoretical and Applied Information Technology*, pages 27–37.

Antunes, M., Maximiano, M., and Gomes, R. (2022). A Client-Centered Information Security and Cybersecurity Auditing Framework. *Applied Sciences*.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., et al. (2009). Above the clouds: A berkeley view of cloud computing.

BSI (2021). IT-Grundschutz-Compendium. Standard, Federal Office for Information Security, Bonn, DE.

Choodakowska, A., Kańduła, S., and Przybylska, J. (2022). Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done. *Lex Localis*.

Cidres, E., Vasconcelos, A., and Leitão, F. (2020). Cloud calculator: a cloud assessment tool for the public administration. In *Proc. of the 21st Annual International Conference on Digital Government Research*, pages 130–137.

Diener, M., Blessing, L., and Rappel, N. (2016). Tackling the cloud adoption dilemma - A user centric concept to control cloud migration processes by using machine learning technologies. In *Proc. of the 11th Int. Conf. on Availability, Reliability and Security (ARES)*, pages 776–785. IEEE.

EU Commission (2022). The Digital Economy and Society Index (DESI).

European Union (2018). Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012.

Feldman, R. (2013). Techniques and applications for sentiment analysis. *Communications of the ACM*, pages 82–89.

Gartner (2022). Umsatz mit Cloud Computing weltweit von 2010 bis 2021 und Prognose bis 2023. Statista.

KonBriefing Research (2022). Statistics: Major cyber attacks on the public sector 1st quarter 2022. Technical report.

Lins, S., Schneider, S., Szefer, J., Ibraheem, S., and Sunyaev, A. (2019). Designing monitoring systems for continuous certification of cloud services: deriving meta-requirements and design guidelines. *Communications of the Association for Information Systems*, pages 460–510.

Markus, H. and Meuche, T. (2022). IT-Sicherheit, Datenschutz und Vergaberecht als Bremsen der Digitalisierung der öffentlichen Verwaltung? In *Auf dem Weg zur digitalen Verwaltung: Ein ganzheitliches Konzept für eine gelingende Digitalisierung in der öffentlichen Verwaltung*, pages 205–242. Springer.

Mell, P., Grance, T., et al. (2011). The NIST definition of cloud computing.

Moses, F., Sandkuhl, K., and Kemmerich, T. (2022). Empirical Study on the State of Practice of Information Security Management in Local Government. In *Proc. of the Conference on Human Centred Intelligent Systems (HCIS)*, pages 13–25. Springer.

Müller, I., Han, J., Schneider, J.-G., and Versteeg, S. (2011). Idea: a reference platform for systematic information security management tool support. In *Prof. of the third Int. Symposium on Engineering Secure Software and Systems (ESSoS)*, pages 256–263. Springer.

Osliak, O., Saracino, A., Martinelli, F., and Dimitrakos, T. (2021). Towards Collaborative Cyber Threat Intelligence for Security Management. In *Proc. of the 7th Int. Conf. on Information Systems Security and Privacy (ICISSP)*, pages 339–346.

Rehbohm, T., Sandkuhl, K., and Kemmerich, T. (2019). On challenges of cyber and information security management in federal structures - the example of german public administration. In *Proc. of the Joint Int. Conf. on Perspectives in Business Informatics Research Workshops and Doctoral Consortium (BIR-WS 2019)*, volume 2443, pages 1–13. CEUR-WS.

Samonas, S. and Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, pages 21–45.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., and Lindgren, R. (2011). Action design research. *MIS quarterly*, pages 37–56.

Stephanow, P. and Banse, C. (2017). Evaluating the performance of continuous test-based cloud service certification. In *Proc. of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, pages 1117–1126. IEEE.

Sterbak, M., Segec, P., and Jurc, J. (2021). Automation of risk management processes. In *Proc. of the 19th Int. Conf. on Emerging eLearning Technologies and Applications (ICETA)*, pages 381–386. IEEE.

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., and Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security*.

Tambou, O. and Pato, A. (2021). Covid-19 vaccination and data protection issues: A european comparative study with focuses on france, germany, belgium, and switzerland. *MPILux Research Paper*.

Taniguchi, T., Maruyama, Y., Kurita, D., and Tanaka, M. (2018). Analysis and classification of university students' educational skills using a computer-assisted web-interviewing questionnaire. *Procedia computer science*, pages 2021–2029.

Wang, T. and Bashir, M. N. (2022). An Analysis of Cloud Certifications' Performance on Privacy Protections. In *Proc. of the 8th Int. Conf. on Information Systems Security and Privacy (ICISSP)*, pages 299–306.