Visualizing the Information Security Maturity Level of Public Cloud Services Used by Public Administrations

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

Keywords: Public Administration, Public Cloud, Visualization, Information Security Management, Security Audit.

Abstract: The digitization of public administrations in Germany is making slow progress. At the same time, more and more innovative IT solutions are available on the market for solving practical business problems, e.g. web-based file sharing applications that are offered by external cloud service providers. Due to data protection regulations and uncertainties regarding information security issues, the adoption and operation of public cloud services within public administrations is a challenging task. As part of our research, we constructed a three-phase process model that uses a web-based tool approach, in order to support chief information officers to manage security audits of various public cloud services that are used by different organizational units. To ensure the efficient, transparent and comprehensive conduction of cloud security audits, we developed graphical visualization components that illustrate the information security maturity level in relation to multiple security requirements of the analyzed public cloud services. We have successfully evaluated our proposed tool visualization under real conditions within a public administration. Furthermore, we discussed several use cases and the user experience with different experts in this application domain.

1 INTRODUCTION

Cloud computing is a trending technology that is nowadays increasingly adopted by government institutions (Mell et al., 2011). The usage of cloud technologies can both reduce ongoing costs of IT expenditures and achieve efficiency advantages. Nowadays, cloud-based IT services offer a wide range of technological options to solve organizational and technical problems efficiently e.g., AWS EC2, Cisco Webex Meetings or Google Workspace. Microsoft 365 is also increasingly being discussed as a possible solution in public authorities, but in its current version it still has numerous conflicts with European data protection regulations (Syynimaa and Viitanen, 2018).

In the recent past, public cloud services have also been increasingly used by public administrations (Nanos et al., 2019). There are many reasons for this. On the one hand, software manufacturers are increasingly tending to offer software products less or not at all for on-premises installations to achieve economies of scale (Armbrust et al., 2009). On the other hand, innovative IT services can be adopted instantly by means of cloud computing, for which previously own high-performance data centers would have been required. In addition, the adoption of cloud services can relieve the organization's IT staff, which is usually necessary for the operation of inhouse IT.

Against the backdrop of the need to massively drive forward the digitization of public administrations in Europe (Braud et al., 2021; European Union, 2018), cloud solutions appear to be a suitable IT solution (Zaharia-Rădulescu et al., 2017; Galletta et al., 2017). For example, smart city projects require powerful IT architectures that support collaboration with various stakeholders (Ge and Buhnova, 2022). The appropriate IT services can be adopted from the cloud so that processing of real-time data becomes possible (Su et al., 2022). In addition, cloud-based IT services can significantly improve the level of IT security, as cloud security experts continuously ensure the implementation of the necessary security measures, thus guaranteeing the protection of entrusted data (Henze et al., 2020).

In most cases, public administrations process personal data in IT systems, sometimes even special categories of personal data (cf. Article 9 EU-GDPR). Consequently, data protection and information security must be considered critically when it comes to processing of sensitive or personal data in public

Diener, M. and Bolz, T.
Visualizing the Information Security Maturity Level of Public Cloud Services Used by Public Administrations.
DOI: 10.5220/0012637700003711

In *Proceedings of the 14th International Conference on Cloud Computing and Services Science (CLOSER 2024)*, pages 192-203
ISBN: 978-989-758-701-6; ISSN: 2184-5042

cloud environments (Rath et al., 2023; Sasubilli and Venkateswarlu, 2021). Although information security and data protection of cloud solutions are highly specified in public tenders, managing the information security of external cloud services is still a major challenge for public administrations (Castro et al., 2019; Nycz and Polkowski, 2015). Furthermore, newly designed and secure federal cloud infrastructures (cf. Bundescloud, Deutsche Verwaltungscloud etc.) are currently not available for small and medium-sized local authorities in Germany. This means that they have to purchase secure public cloud services themselves, which increases the risk of security gaps immensely.

The issue that the management of information security in public authorities is inadequate is shown by the fact that there have been approximately 100 documented IT attacks on public authorities in Germany between 2020 and 2024 (Lange, 2024). Not all of them have been successful, but the sheer number of attacks shows how dramatic the trend is among German authorities.

As a result of the increasing adoption of public cloud services in public administrations, it must be assumed that there will be an expansion of data breaches or cyberattacks. Suitable practical solutions for securing public cloud services in the area of public administrations are currently indispensable.

This paper proposes a possible technical solution that can support responsible actors in public administrations to enhance the required information security maturity level for used public cloud services by offering advanced visualization techniques based on realtime audit information.

The remainder of this paper is organized as follows: In the next section we describe practical problems of public administrations with respect to information security management of public clouds using the example of a medium-sized municipality. In the related work part we describe how visualization grids can be used to highlight anomalies in security configurations (cf. section 3). In section 4, we propose a process model that describes how tool-guided audits with focus on public clouds in a municipality can be implemented into information security processes. Based on this, we present our developed prototype, which provides visualization grids for highlighting anomalies due to organizational and technical security requirements within public clouds (cf. section 5). Following, we evaluate the proposed prototype in section 6. Based on this, we discuss in section 7 the evaluation results and the user experience of our developed prototype with experts from different public administrations. In the last part of the paper, we summarize the results of our work and provide an outlook.

2 BACKGROUND

One of the authors is chief information security officer (CISO) of a medium-sized municipal government and has deep insights into information security processes. Since the beginning of the Covid-19 pandemic in spring 2020, observations have been ongoing regarding the adoption, the implementation, and the usage of public cloud services in its public administration.

2.1 Unclear Responsibilities and Changing Structures

Basically, the expectations of implementing cross-organizational IT solutions to drive digitization forward, have increased dramatically. In particular, the number of cloud applications has massively increased, as less internal resources (e.g., IT technology, personnel) are necessary compared to on-premises applications. In contrast, the responsibility for managing external cloud services lies with those departments that originally request the cloud service. However, the problem is that employees in requesting departments often have little or no IT expertise, that leads to serious gaps in information security processes. To make matters worse, SaaS applications in clouds are often multi-tenant and can be used in various departments under different responsibilities. This makes it increasingly difficult to keep track of the adopted cloud solutions within public administrations. As a result of changes in departmental responsibilities, it can happen that the organizational and technical administration of public clouds are not carried out to the necessary degree as they are required by security requirements of standards (e.g., ISO 27001, BSI C5, CSA CCM, BSI IT-Grundschutz, CISIS12 etc.)

2.2 Security Audits of Public Clouds Services

Today, many SaaS products do not offer an OpenID interface, so that a single-sign-on (SSO) against a user directory like Active Directory is technically unfeasible. Since many different public cloud services are adopted by public administrations, it is difficult to use standardized APIs. As a consequence, public cloud services have their own identity management that needs to be controlled manually.

If these manual identity checks are not carried out carefully, serious security gaps can arise in identity management processes. In a worst-case scenario, former employees could have full access to sensitive data

in public clouds, which they should no longer have. In addition, the activation of important security configurations in each tenant of a public cloud service is of particular importance. For example, the password quality requirements must be correctly configured by the responsible manager of a public cloud service.

In general, the problem is that such security checks must be done manually under these circumstances and need to be done regularly for the identified public cloud services. In this respect, the only option for CISOs might be to ask the responsible cloud managers about the compliance of the defined organizational security requirements. However, these organizational security requirements are extremely difficult to implement in practice.

3 RELATED WORK

3.1 Visualization of Information

The possibilities of visualizing data relationships have been researched for a long time and support a wide variety of presentation techniques (Mazza, 2009). Increasingly, visualization techniques are being used to support decisions in information security processes by presenting complex relationships in simplified presentations (Yermalovich, 2020). As a consequence it becomes possible to illustrate complex correlations of business processes, system configurations etc. For example, Colantonio et al. developed a grid based visualization technique which has simplified the understanding of roles in social networks (Colantonio et al., 2011). In their proposed approach, they visualized existing access permissions between users and objects using a two-dimensional grid (Meier et al., 2013). With the help of visual grids, complex data representations can be depicted graphically. Item series A is assigned to the x-axis, while item series B is assigned to the y-axis (cf. figure 1).

x-axis

y-axis		item A1	item A2	item A3	item A4	item A_n
	item B1	x		x	x	
	item B2		x		x	
	item B3		x			
	item B4			x	x	
	item B_n					

Figure 1: Grids are able to represent two-dimensional relations of data.

If there is any relationship between two items, it can be easily presented by a simple cross. The statement about the relationship between two characteristics can then be depicted in a cell, e.g., by a numerical value or a colored representation. For our research we will adapt the principles of this visualization technique. Heatmaps are sophisticated visualizations with which multidimensional facts can be presented. These are not required for our work.

3.2 Security Audits of Public Cloud Services

The maturity level of information security can be determined by adapting different methods (Proença and Borbinha, 2018; Jaatun et al., 2017). A widespread approach bases on questionnaires (Schmitz et al., 2021). The status quo is documented in relation to specific information security requirements (Parsons et al., 2017). Depending on the design of the questions, an automated evaluation of the answers can take place. Typically, information security management tools (e.g., eramba[1], verinice[2]) support CISOs in managing technical and organizational security requirements.

A highly simplified and ubiquitous approach for auditing public cloud services is based on validity checks of their underlying certifications (cf. ISO 27001). The problem with this audit approach might be that it is not possible to validate organizational security processes at the cloud customer side (Di Giulio et al., 2017). For example, the quality of identity management processes cannot be expressed by cloud certificates. Lins et al. are exploring the approach of dynamic cloud certification (Lins et al., 2019). By applying this form of auditing, standardized measurement indicators are regularly queried and evaluated, e.g. the availability of the cloud over time. In this respect, it is possible to monitor promised service level agreements (SLAs) during operation (Stephanow and Fallenbeck, 2015). However, by using this dynamic approach it is also difficult to automatically check semantic relationships, for example, the allocation of access rights to cloud users.

Recently published research has focused on methods with multi-dimensional certification to handle user's requirements on the full public-cloud-services life cycle (Anisetti et al., 2023).

[1] https://www.eramba.org
[2] https://verinice.com/en

4 CONCEPTUAL DESIGN: EFFICIENT CLOUD SECURITY AUDITS IN PUBLIC ADMINISTRATIONS

Our approach is based on the idea of conducting organization-wide security audits in different departments which have adopted public cloud services. Security audits in public administrations must be simple and efficient, so that regular repetitions are accepted by the involved actors. By iteratively applying the principles of the design science research (DSR) method (Peffers et al., 2007), we developed a three-phase process model, with the goal of determining the maturity level of information security:

- **Phase 1: Inventorying Existing Public Clouds.** As a first step, we conduct a inventory of all public cloud services in each department. We also determine who is responsible for the management of the respective cloud. This step is performed for each organizational unit of the public administration by asking skilled employees.
- **Phase 2: Auditing the Public Cloud Security.** The used public cloud services are then examined more precisely. It is important that cloud services are audited per organizational unit, as different organizational conditions and settings can be given. The answers of phase 1 serve as starting point.
- **Phase 3: Evaluating the Cloud Information Security Maturity Level.** Based on the questions answered in phase 2, the maturity level of information security is determined for each organizational unit for each adopted public cloud service. In this step, deviations and anomalies are identified by using graphical visualizations.

As part of the DSR design cycle, we discussed with various stakeholders in six different public administrations, including chief information officers, data protection officers and e-government managers. Additionally, we discussed with several heads of various departments of our own public administration. During this process, we were able to identify three different roles that are mandatory to perform information security audits of public cloud services within public administrations successfully. Each of the actors involved is taking on activities that are mapped to the proposed three-phase process model. Figure 2 illustrates in BPMN 2.0 notation the holistic process of security audits of public cloud services within a public administration and the respective activities of the actors involved.

In general, it is essential that all incoming and outgoing audit information is stored within a central repository. This ensures that audit data is captured in a structured way and is reusable for different activities. In addition, it is important to involve the management of each organizational unit in the audit process as early as possible. In this context, we explain why security audits are necessary for public cloud services and for what reason employees of a department need to be involved. In terms of conducting cloud security audits in public administrations, we identified the following actors and activities:

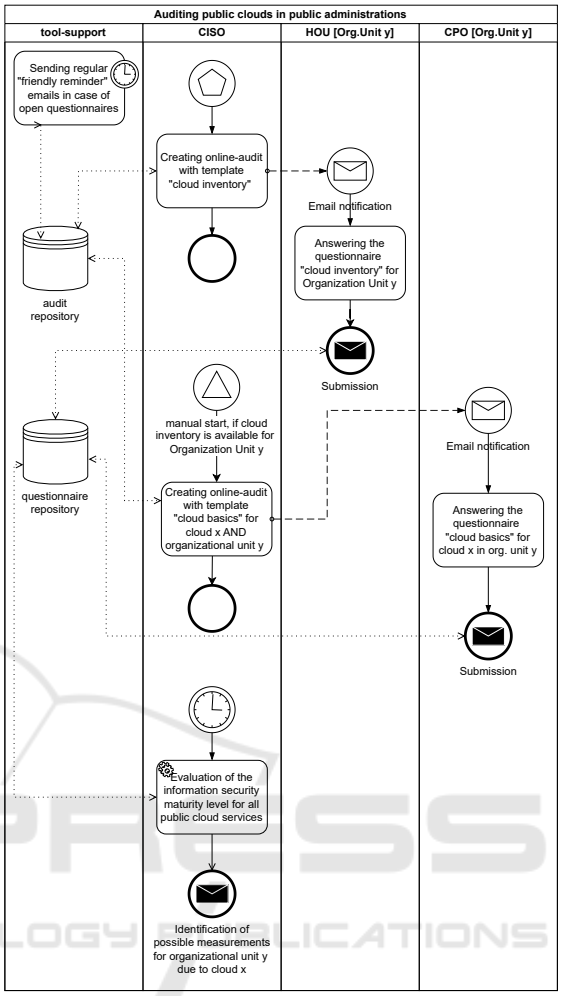

Figure 2: Holistic process of cloud security audits within public administrations.

- **CISOs** are responsible for the central management of all information security audit and are significantly involved in the activities of the three phases. For this purpose, the respective heads of the organizational units (HOUs) need to be identified and documented in phase 1.
- **HOUs** themselves determine for their organiza-

tional unit which cloud services are being used and which employees are responsible for their management in each case. The answers are submitted to the CISO in a structured form. The employees, that are responsible for administrative cloud management activities are called Cloud Product Owners (CPOs).

- **CPOs** answer specific audit questions that are related to the public cloud services for which they are responsible. Moreover, in many cases they are responsible to implement security measures in their application field. Due to the involvement of HOUs in individual organizational units, a seamless relationship between CISOs and CPOs can be easily established.

Overall, it becomes clear that a comprehensive tool support is necessary to apply the proposed process model in the domain of public administrations. During the DSR cycle, we conducted several interviews thus we could identify three key requirements that are essential for enhanced tool support:

1. It must be immediately apparent which organizational unit uses specific public cloud services.
2. In addition, the status of the initiated security audits must be traceable.
3. It must be apparent to what extent specific security requirements of public cloud services are implemented.

4.1 Analysis of Existing Audit Software

In this context, we also looked at three different proprietary security tools that are common and currently used by CISOs in their public administrations.

It was noticeable that all three tools were used exclusively by CISOs due to their enormous range of functions. In all cases, user training would be necessary to provide CPOs with the necessary basic understanding of how to use the questionnaires. In addition, full licenses are always required for the use of online questionnaires in the tools, meaning that the number of cloud audits that can be carried out in parallel is likely to be low.

None of the three tools examined have a workflow engine that would support the integration of HOUs. This results in additional coordination effort for CISOs, as additional tools would have to be used in the process model. In a highly dynamic cloud environment, this is a disadvantage for the analysis of information security.

Furthermore, the CPOs' responses in the questionnaires could not be evaluated automatically. This additional activity would have to be carried out by CISOs, which would likely mean that cloud audits would not be repeated on a regular basis.

Two of the tools examined do not have a web-based interface, which presents an additional difficulty in large structures of public administrations. One tool enables the use and customization of dashboards, but only data that is known can be visualized. Missing data cannot be visualized as an anomaly in this dashboard.

Altogether, we found that the process model we proposed can only be supported to a limited extent by established tools. A subsequent search on the internet for cloud audit tools was also of little help in solving the identified challenges in the public authority environment.

5 PROTOTYPE: VISUALIZING THE INFORMATION SECURITY MATURITY LEVEL OF PUBLIC CLOUDS

Following, we present the basic considerations of our proposed tool which provides the proposed holistic process for conducting decentralized security audits of public cloud services within public administrations. The development cycle took place over several months since 2022 and, in accordance with the DSR principles, required a mutual comparison with practical requirements and the scientific literature. Our goal was to achieve a practical solution that is able to support the mentioned process model in order to determine the information security maturity level of public cloud services.

During our research work, we have considered the relevance and the rigor cycle in accordance with the DSR principles. On the one hand, we searched the literature for suitable approaches, and on the other hand, we always compared them with the actual problem and discussed them with various actors involved in the security audit process. During the expert discussions, we identified the following essential requirements that a novel tool approach must provide:

- **Self-explanatory Graphical User Interface:** The web-based questionnaire had to be designed in such a way that no further education and training of individual actors is required.
- **Automatic Single Sign-On:** Respondents do not have to manually log in to our prototype. Instead, user authentication uses a kerberos mechanism. This keeps the barriers for answering questionnaires as low as possible.

- **Multiple-Choice Answer Options:** In order to be able to carry out the online questionnaires efficiently and in a standardized manner, descriptive text answers should be avoided as far as possible. Instead, answers are pre-qualified so that they can later be analyzed automatically to determine the information security maturity level.
- **Automatic Storage of Answers:** To avoid data loss during the execution of more comprehensive audits, the answers given should be stored temporarily. This will significantly increase the user experience and acceptance of our tool during the entire security audit.
- **Delegation of the Questionnaire:** Employees who receive a web-based questionnaire should themselves be able to forward them to more suitable persons. This should avoid unnecessary routing times.

5.1 Technical Specifications

Our prototype runs on-premises on a virtualized Ubuntu Linux server (8 GB RAM, 30 GB disc space) with access to internal network resources of our authority. Access to this server is only possible from the internal network for security reasons.

We have used Apache[3] web server, MySQL[4] database, as well as Laravel[5] and Laravel-Livewire[6] programming frameworks to build our prototype.

The access to the collected data and visualizations in the tool is limited, depending on the user's role. We have currently implemented three roles: CISO, HOU and CPO. The CISO role is the only one with administrative rights and full access to the data. Users who are assigned the HOU or CPO roles only see the data records released for them for an organizational unit or for the assigned cloud assets. The answers of the questionnaires are transmitted in encrypted form. The database access is restricted so that only administrators and service users can use the raw data.

5.2 Preparation of Cloud Audits

Before our proposed process model can be applied for cloud security audits, the underlying questionnaire must first be modeled in our prototype. We focus on the ISO 27001 standard to formulate appropriate questions about cloud security requirements. In a previous published research paper (Diener and Bolz, 2023), we have already successfully proven the utilization of multiple-choice answers with associated sentiment levels. Based on the concept of predefined sentiment levels, we can create precise statements about the information security maturity level of a specific public cloud service. Each cloud audit relates to a single organizational unit. Thus, it is possible to identify possible lacks of security requirements automatically, if answers with negative sentiments are given by CPOs. In addition, it is possible for CISOs to predefine suitable security measures that can be automatically derived in case that negative sentiments were identified. Figure 3 shows the question wizard in our prototype that allows CISOs to qualify predefined multiple choice answer options with a machine readable sentiment.

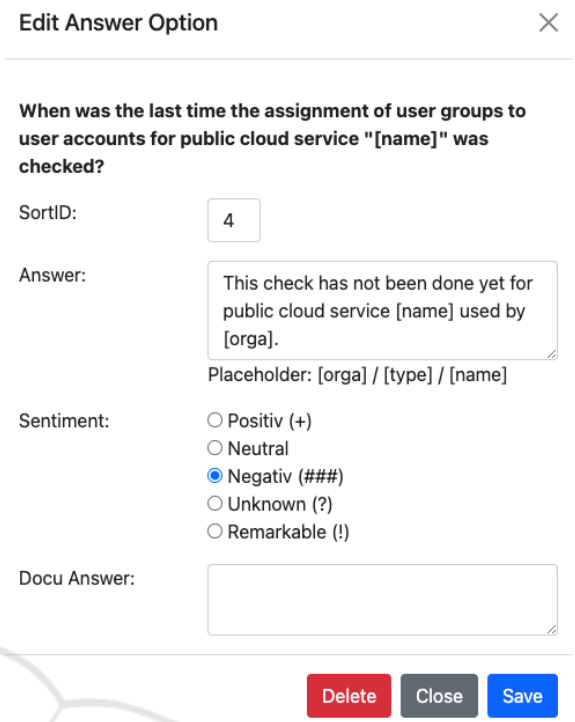

Figure 3: Predefinition of one sentiment for one of several answer-options to a single question.

By submitting predefined web questionnaires to the appropriate actors, CISOs can initiate follow-up security audits in different organizational units with respect to phases 1 and 2 of our proposed process model. For example, general questions about adopted public cloud services are submitted to HOUs of organizational units. The given answers will be manually checked by the CISO. Based on the received results, phase 2 is initiated by the CISO for the identified public cloud services. Consequently, responsible CPOs will obtain automatically generated questionnaires with placeholders of public cloud services for

[3]https://httpd.apache.org
[4]https://mysql.com
[5]https://laravel.com
[6]https://laravel-livewire.com

which they are responsible. This means that the effort required to provide individual questionnaires is very low. At all times, the CISO maintains full control over all running cloud security audits with the help of our prototype.

5.3 Managing Security Audits

As the number of concurrent security audits for public cloud services is growing fast in large organizations, it becomes increasingly difficult for CISOs to keep track of all running activities. Although it is possible to export metadata of audits for data analysis to external tools such as Microsoft Excel, enormous time efforts will be associated. Moreover, there is no processing of real-time data, as audit states can change very quickly in heterogenous organizations.

Consequently, a graphical visualization of the current state of security audits and the corresponding relations between organizational units and public cloud services is required. To solve this problem, we propose the usage of a two-dimensional visualization grid that represents the relationships between organizational units and their adopted public cloud services within a public administration (cf. figure 4). We name this component organizational units assets grid (OAG).

By using this visualization technique, CISOs obtain a realtime overview about the adopted public cloud services within their organization. Conversely, it becomes obvious for which public cloud services and organizational units no relationship is existing (e.g., red font color). In such cases, our developed graphical visualization supports CISOs to identify possible missing correlations at a glance.

Additionally, the background color of single cells provides information about the status of the intended security audits. Marked cells in *red* mean that no audit has yet been initiated for this relation. In such situations, it is highly likely that phase 1 of our process model must be carried out first. The *orange* color indicates that a initiated security audit is still running. Finally, *green* colored cells indicate that the audit for a specific public cloud service in an organizational unit has been finished and no further activities are required by the involved actors. Marked cells in *white* signal that there is no proven relation existing between a single organizational unit and a public cloud service.

Moreover, we developed an additional visualization grid for our prototype, supporting a simplified visual determination of the maturity level of information security for the adopted public cloud services. For this purpose, the answers from the submitted questionnaires are automatically evaluated. Based on the predefined sentiment level of each answer, a graphical visualization is dynamically generated. In the following section, we explain the concepts of this novel functionality.

6 EVALUATION

In this section, we present the results of the evaluation of the developed visualization grids that are implemented in our prototype. For the evaluation we have chosen a real use case from practice in our public administration. We focus on auditing four different public cloud services used by five different schools in order to determine the maturity level of information security.

Four of the five schools report directly to our Public Administration e.g., three professional schools and one high school. These organizational units must follow the CISO's instructions, such as participating in the analysis of the status quo of their individual information security maturity level. One of the twenty elementary schools in our city is also participating in the evaluation but is not subject to instructions from our Public Administration. This means that we have selected an appealing and realistic scenario for our evaluation, which we understand well. The validity of the information presented in the visualization grid can thus be checked easily and quickly.

The evaluation of the application of both visualization grids is based on the process model we presented in section four. In phase 1, we used a web-based questionnaire in our audit tool to determine which public cloud services are adopted by the five schools. Following the process model, we surveyed the principals of the schools for phase 1. Responses were available the next business day from all schools. Once all responses were received, we were able to evaluate the OAG visualization that we have developed.

6.1 OAG Visualization

The OAG provides an overview of the existing relations between the audited organizational units and their adopted public cloud services (cf. figure 4). For a better data presentation in our visualization grid, the filter was set to the asset type "cloud". By applying the OAG visualization in our prototype, we were able to identify the following key facts in phase 1:

- Very quickly, we found that Public Cloud 2 is stored in our repository but is not used by any of the schools surveyed. The OAG marks this fact with a red font color.

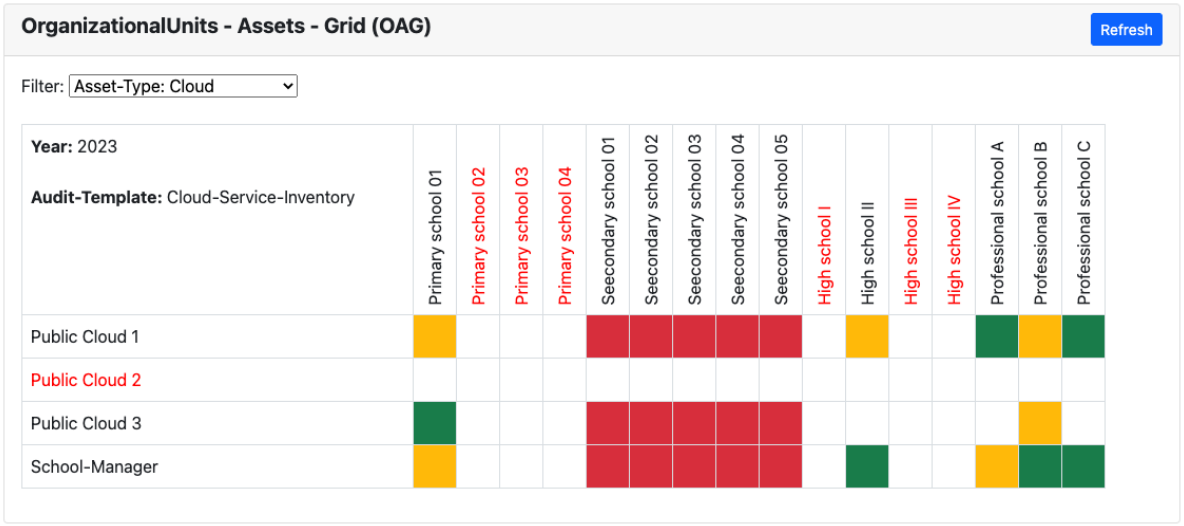

Figure 4: Visual managing support of cloud security audits within public administrations.

- Three of the twenty elementary schools and three other high schools that do not report to our public administration are already documented in our audit tool. Six schools of the listed organizational units do currently not have an assignment to a public cloud service (cf. red font color).
- Immediately it becomes clear that five secondary schools are already documented in our audit tool, for which a relation to Public Cloud 1, Public Cloud 3 and School Manager is existing. Since no audit was allowed to be started for these schools yet, the cells are red colored in each case.
- The OAG visualization shows that six audits are currently still running (cf. orange cells) and six audits have already been completed (cf. green cells) with respect to the questionnaire of phase 1.

Overall, we have found that the OAG visualization is suitable for monitoring the status quo for several security audits running in parallel. It is important to use filters, otherwise the clarity suffers when different asset types are displayed.

6.2 Visualizing the Information Security Maturity Level

Based on phase 1, the subsequent phase 2 focuses more detailed on ISO 27001 security requirements for all public cloud services used by different organizational units (*green* marked). Therefore, the cloud product managers (CPO) receives personalized questionnaires. Since high-quality data has already been collected in phase 1, a targeted initiation of security audits is possible. Similar to their superiors (HOUs), the CPOs receive automatically generated emails with a link that leads directly to the online questionnaire. A total of 10 different CPOs received a questionnaire at the five schools (cf. figure 5). The number is so high because at each school exactly one teacher is responsible for one single public cloud service. One exception is Primary school 01: the principal is responsible for managing all cloud services herself.

The most important finding in the context of this evaluation was that teachers at the schools were partly unaware that they themselves were responsible for the information security measures of the adopted public cloud services. In some cases, the CPOs thought that the IT department of the public administration or the cloud service provider itself is responsible for managing the information security. In addition, there was a lack of clear understanding of what activities information security encompasses. In this respect, the structured questionnaire in our audit tool indirectly helped to raise the awareness of information security activities among the CPOs involved.

After five working days, we evaluated the answers of the submitted questionnaires using our designed security requirement grid (SRG). The SRG is structured similarly to the OAG. We will briefly describe the differences here. In the SRG, the x-axis represents the public cloud services used by an organizational unit. In the first line of the grid, these are summarized in groups. For example, only two public clouds are assigned to High school II. The security requirements checked in each case are listed on the y-axis in the SRG. These are grouped according to the main requirements. In the cells of the SRG visualization, five different color types represent the state of the information security maturity level. The colors correlate

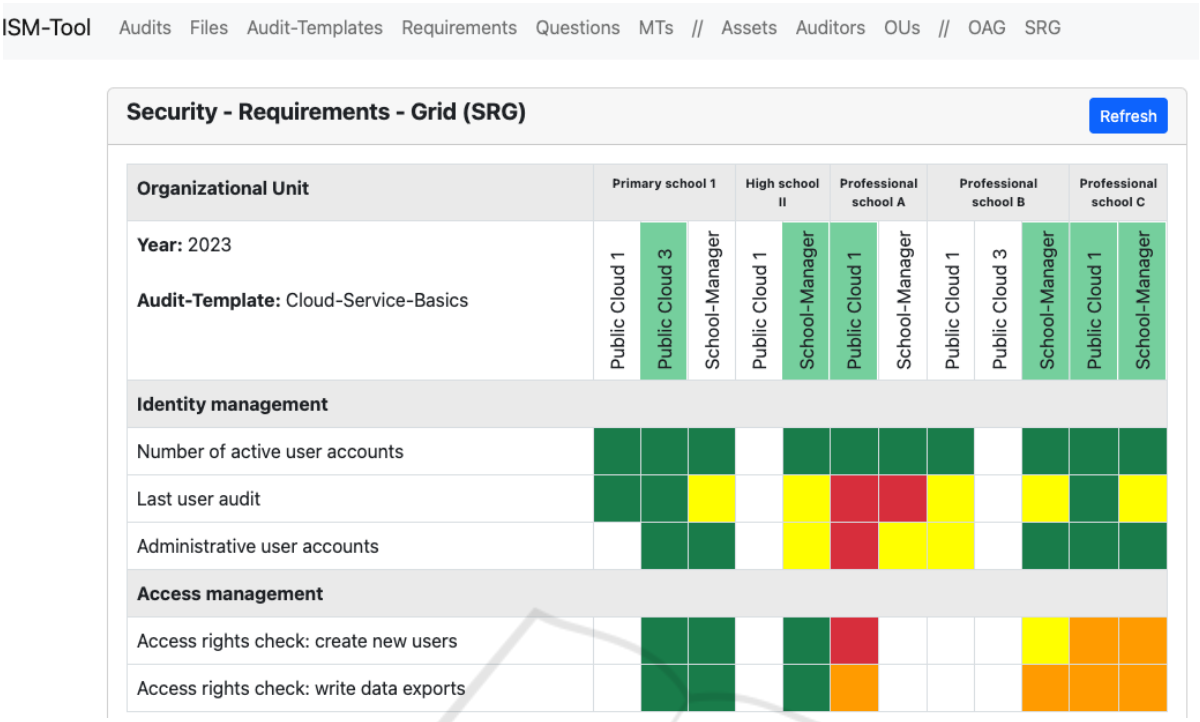

Figure 5: The SRG visualizes the information security maturity level of different public clouds.

with the sentiment of the associated responses of the questionnaires. Positive and neutral sentiments are represented in *green* color. Answers with negative sentiment are marked in *red*. Remarkable sentiment is visualized in *yellow*. Unclear answers from respondents are colored *orange*. Unanswered questions are shown in *white*.

In the course of phase 3 of our proposed process model, we checked the relevance and correctness of the information presented in the SRG visualization. Overall, our questionnaire on cloud security consisted of two groups of topics. Group one focused on the status quo of identity management and group two on the authorization concept based on it. In the following, we describe the most important key findings of the evaluation of the SRG visualization:

- The organizational units (cf. second row) highlighted in *light green* indicate that the associated security audits have been completed. This level of information is identical to the OAG visualization.
- Public Cloud 3, which is used in Primary school 1, has a very high maturity level in terms of information security. Public Cloud 1 used by Professional school A has the worst maturity level for information security. Three security requirements obtain a negative sentiment, e.g. the question about the last check of user accounts. Of particular concern in this context is the fact that the access rights for creating new users are obviously incorrect. In addition, it is not clear to the responsible CPO to what extent the permissions for data export are set correctly. For the CISO it becomes clear, that there is needed an urgent improvement in this school with respect to Public Cloud 1, for example by conducting some security management trainings.
- Overall, it is noticeable that the questions about access rights at the vocational schools were frequently provided with unclear answers. This could indicate that the responsible CPOs are also insufficiently trained on this topic. A direct inquiry by the CISO will bring clarity.
- In addition, it is clear that numerous responses from Professional school A and B as well as High school II for Public Cloud 1 are currently missing. Reminder emails could be sent automatically by our prototype to the respective responsible CPOs to speed up the audit process.

In total, we have not been able to identify any errors in the representations of the status quo of the OAG and SRG visualizations, displaying the information security maturity level of a selected organizational units. At the same time, the CISO gained valuable insights in the status of the information security maturity level of the public cloud services, that are used by organizational units within the public administration.

7 DISCUSSION

Based on the aforementioned evaluation results of our prototype, we initiated a discussion about the findings with HOUs and CPOs of our authority. Furthermore, we discussed the results with five CISOs from different public administrations in order to improve the proposed prototype and to make scientific contributions to user experience aspects.

Basically, the proposed **tool support is simple and self-explanatory**. It is noticeable that there are few icons on the GUI, so that CISOs are not overwhelmed. Comprehensive training is therefore not required. The advantage is that CISOs can use the tool to manage all security audits centrally, although the use of public cloud services is decentralized and carried out independently in the offices by various CPOs. The integration of mail information has proven to be very useful, as the responsible CPOs can be regularly reminded of open audits using friendly-reminder.

The OAG visualization is useful compared to established dashboards in ISMS tools, as it is possible to see **at a glance which cloud department relations have not yet been audited**. This significantly improves the level of information security in an authority. It is not necessary to add filters to traditional reports. In addition, this grid approach visualizes every possible relationship between department and public cloud service. However, the grid becomes very unwieldy as soon as many departments are entered in a large authority.

Looking at the SRG visualization, it became clear that it is **very easy to determine the maturity level of information security**, as it is possible to see at a glance which of the public cloud services used have serious weaknesses in the security requirements based on the colored markings. For example, cells marked red in the SRG show that negative or even critical answers were given by the CPOs to the questions asked. This is very helpful for CISOs, as there is no need to read comprehensive reports. Instead, the CISOs can make direct enquiries to the CPOs. Compared to the usage of traditional tools, it is necessary to manually identify each organization-cloud relationship and then define the corresponding security requirement questions. This is not necessary with the tool we presented and was rated positively by the CISOs interviewed.

In general, it was positively noted that the question texts can be easily individualized with our prototype by integrating the product names of individual cloud services. We use placeholders in the question texts for this purpose (cf. figure 3). This **increases the respondents' awareness of the audited context** when they have to deal with the confronting questions. As a result, CPOs always have a concrete reference to the currently audited public cloud service during the audit. This is particularly useful if several public cloud services are used within an organizational unit. This fact was particularly confirmed from the perspective of CPOs.

CPOs themselves were also impressed by the fact that login to the questionnaire is very low-threshold thanks to SSO authentication via Kerberos ticket. This **eliminates time-consuming registration and login processes**, which users often fail at if they only work with the audit questionnaire once or twice a year.

The fact that the additional collected data from the questionnaires is stored in a separate database was seen as a negative factor. As most public administrations already use tools for information security management, inconsistencies may arise between the two systems. For this reason, it was suggested that an **API should be developed to enable data exchange** between our prototype and existing security tools.

8 CONCLUSION

In this work, we extended our web-based audit tool with two visualization grids, supporting CISOs in public administrations with realtime information about the maturity level of the information security with respect to the adopted public cloud services within different organizational units. The development of the visualization grids took place in several cycles by adapting the DSR process with different internal and external stakeholders. The evaluation of the developed OAG and SRG visualizations was done by investigating a practical example within our public administration. Additionally, we discussed the evaluation results with CISOs from different authorities in order to achieve deep feedbacks to our research.

In general, our research has shown that traditional software products for security audits have reached their limits when it comes to auditing decentralized public cloud services in public administrations. Innovative and lightweight concepts are essential in this domain to ensure the information security of public cloud services in public administrations in the future. In particular, the knowledge carriers in the respective departments must be intensively involved in both the security processes and the use of audit tools.

Moreover, we were able to show that it is possible to implement more efficient and transparent security audit processes by using novel visualization techniques. With the help of our enhanced tool, holistic

information security processes in public administrations can be improved, so that the management of decentralized public cloud services becomes possible. This research work has found out three key findings:

1. The proposed OAG visualization provides a simple overview of the identified public cloud services and existing departments in an organization. A relation between them is described by using colored cells. CISOs can easily use this feature to obtain a quick overview about the status of various security audits of different assets within an organization. Traditional reports and dashboards have the problem that anomalies can only be displayed to a limited extent.
2. While designing the procedure for our three-phase process model, we were able to identify three important actors for conducting security audits of public cloud services within public administrations. The CISO himself is the main actor and needs to be able to coordinate security audits by using novel visualization techniques. HOUs of organizational units need be involved immediately and in an easy way, to obtain meta information about responsibilities with respect to adopted public cloud services. The people actually responsible for public clouds (= CPOs) must be directly involved in security audits, as a public administration's IT department is often not responsible for supporting decentralized public cloud services.
3. In practice, similar public cloud services are used by different departments within an organization. Therefore, the relationships between organizational units and the adopted public cloud services must be documented at regular intervals. New audits can then be generated on the basis of visualized anomalies (cf. Figure 4). As a consequence it is possible to derive the maturity level of information security with respect to concrete security requirements (cf. Figure 5) by using visualization techniques.

In future research we want to achieve further improvements in this research field. For example, the problem of potential shadow IT needs to be investigated. In this context, we want to make scientific efforts to train HOUs to identify public cloud services in their departments. If a new, previously undocumented cloud has been identified, the further ISMS process should be carried out in a lightweight manner with the help of our tool.

In addition, we want to find out how our web-based audit tool can be combined with security awareness methods. We have noticed during our security audits that despite previous e-learning trainings on security awareness, there is still a lack of understanding with regard to security measures within public cloud services. Moreover, we would like to evaluate the practical applicability of our developed tool under real conditions in another authority. We want to understand to what extent visualizations can help CISOs to improve the maturity level of information security. For this reason, we will attempt to carry out a quantitative analysis in collaboration with another authority over a longer period of time in which metrics are examined in order to be able to make statements about the effectiveness of our prototype. However, this project is associated with major hurdles in the authorities' environment.

There is also the problem that CPOs may give incorrect answers in the questionnaires because they do not understand the context properly. In this respect, we need to make further observations to assess the extent to which qualitatively complete and correct answers to questions are reported back.

Taking everything into account, we are making the public administration sector a bit more secure, and we are helping to drive forward the urgently needed implementation of digitization in this environment.

REFERENCES

Anisetti, M., Ardagna, C. A., and Bena, N. (2023). Multi-dimensional certification of modern distributed systems. *IEEE Transactions on Services Computing*, 16(3):1999–2012.

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.

Braud, A., Fromentoux, G., Radier, B., and Le Grand, O. (2021). The road to European digital sovereignty with Gaia-X and IDSA. *IEEE Network*, pages 4–5.

Castro, K., Macedo, G. R., Araujo, A. P., and de Carvalho, L. R. (2019). Cloud. jus: Architecture for provisioning infrastructure as a service in the government sector. In *Proc. of the 9th Int. Conf. on Cloud Computing and Service Science (CLOSER)*, pages 412–421.

Colantonio, A., Di Pietro, R., Ocello, A., and Verde, N. V. (2011). Visual role mining: A picture is worth a thousand roles. *IEEE Transactions on Knowledge and Data Engineering*, 24(6):1120–1133.

Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R. H., and Bashir, M. N. (2017). Cloud standards in comparison: Are new security frameworks improving cloud security? In *Proceedings of the 10th Int. Conf. on Cloud Computing (CLOUD)*, pages 50–57. IEEE.

Diener, M. and Bolz, T. (2023). Cloud inspector: A tool-based approach for public administrations to establish information security processes towards public clouds.

In *Proc. of the 9th Int. Conf. on Information Systems Security and Privacy (ICISSP)*, pages 543–551.

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.

Galletta, A., Ardo, O., Celesti, A., Kissa, P., and Villari, M. (2017). A recommendation-based approach for cloud service brokerage: A case study in public administration. In *Proc. of the 3rd Int. Conf. on Collaboration and Internet Computing (CIC)*, pages 227–234. IEEE.

Ge, M. and Buhnova, B. (2022). Disda: Digital service design architecture for smart city ecosystems. In *Proc. of the 12th Int. Conf. on Cloud Computing and Service Science (CLOSER)*, pages 207–214.

Henze, M., Matzutt, R., Hiller, J., Mühmer, E., Ziegeldorf, J. H., van der Giet, J., and Wehrle, K. (2020). Complying with data handling requirements in cloud storage systems. *IEEE Transactions on Cloud Computing*, 10(3):1661–1674.

Jaatun, M. G., Tøndel, I. A., Moe, N. B., Cruzes, D. S., Bernsmed, K., and Haugset, B. (2017). Accountability requirements for the cloud. In *Proc. of the 8th Int. Conf. on Cloud Computing Technology and Science (CloudCom)*, pages 375–382. IEEE.

Lange, J. (2024). Kommunaler Notbetrieb: IT-Sicherheitsvorfälle in Kommunalverwaltungen. https://kommunaler-notbetrieb.de.

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.

Mazza, R. (2009). *Introduction to information visualization*. Springer Science & Business Media.

Meier, S., Fuchs, L., and Pernul, G. (2013). Managing the access grid-a process view to minimize insider misuse risks. In *Proc. of the 11th Int. Conf. on Wirtschaftsinformatik (WI2013)*.

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

Nanos, I., Manthou, V., and Androutsou, E. (2019). Cloud computing adoption decision in e-government. In *Operational Research in the Digital Era–ICT Challenges: 6th International Symposium and 28th National Conference on Operational Research, Thessaloniki, Greece, June 2017*, pages 125–145. Springer.

Nycz, M. and Polkowski, Z. (2015). Cloud computing in government units. In *Proc. of the 5th Int. Conf. on Advanced Computing & Communication Technologies*, pages 513–520. IEEE.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., and Zwaans, T. (2017). The human aspects of information security questionnaire (hais-q): two further validation studies. *Computers & Security*, 66:40–51.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, 24(3):45–77.

Proença, D. and Borbinha, J. (2018). Information security management systems-a maturity model based on iso/iec 27001. In *Proc. of the 21st Int. Conf. of Business Information Systems (BIS)*, pages 102–114. Springer.

Rath, M., Keller, L., and Spies, A. (2023). Sovereign clouds—an overview of the current privacy challenges associated with the use of us cloud services, and how sovereign clouds can address these challenges. *Computer Law Review International*, 24(3):78–84.

Sasubilli, M. K. and Venkateswarlu, R. (2021). Cloud computing security challenges, threats and vulnerabilities. In *Proc. of the 6th Int. Conf. on Inventive Computation Technologies (ICICT)*, pages 476–480. IEEE.

Schmitz, C., Schmid, M., Harborth, D., and Pape, S. (2021). Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities. *Computers & Security*, 108:102306.

Stephanow, P. and Fallenbeck, N. (2015). Towards continuous certification of Infrastructure-as-a-Service using low-level metrics. In *Proc. of the 12th Int. Conf. on Ubiquitous Intelligence and Computing (UbiComp)*, pages 1485–1492. IEEE.

Su, P., Chen, Y., and Lu, M. (2022). Smart city information processing under internet of things and cloud computing. *The Journal of Supercomputing*, pages 3676–3695.

Syynimaa, N. and Viitanen, T. (2018). Is my office 365 gdpr compliant?: Security issues in authentication and administration. In *International Conference on Enterprise Information Systems*. SCITEPRESS Science And Technology Publications.

Yermalovich, P. (2020). Dashboard visualization techniques in information security. In *Proc. of the 7th Int. Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–6.

Zaharia-Rădulescu, A.-M., Radu, I., et al. (2017). Cloud computing and public administration: approaches in several european countries. In *Proc. of the Int. Conf. on Business Excellence*, volume 11, pages 739–749. Sciendo.