Universität Regensburg
Fakultät für Wirtschaftswissenschaften
Institut für Wirtschaftsinformatik

Managing Information Security of Public Clouds for E-Government

Dissertation

zur Erlangung des Grades eines Doktors der Wirtschaftswissenschaft,
eingereicht an der Fakultät für Wirtschaftswissenschaften der Universität Regensburg

vorgelegt von:

Michael Diener, M.Sc. with Honors

Berichterstatter:

Prof. Dr. Hans-Gert Penzel

Prof. Dr. Günther Pernul

Tag der Einreichung: 30.08.2024
Tag der Disputation: 18.03.2025

Abstract

At the moment, public administrations are forced to integrate public cloud services into their internal networks due to the digital transformation (e.g. AI services, collaboration, e-government, etc.). Therefore, information security management must be intensified in order to comply with confidentiality, availability, integrity and data protection regulations. Although a wide range of methods, concepts and tools for cloud security have been researched and established, there is a lack of suitable management processes for information security of public clouds in this application domain among practitioners and academics. As a result, this dissertation focuses on cloud security management, cloud audits and cloud utilization. For this purpose, a dynamic process model with tool support is developed in order to systematically improve information security for adopted public cloud services in the domain of public administrations. In addition, empirical data is collected on the utilization of public cloud services in German municipal administrations and the status quo of information security. The results clearly show that public cloud services are used intensively in public administrations at municipal level, but that there are considerable deficiencies in information security concepts. The artifacts of this work make a scientific and practical contribution towards improving the resilience of digital transformation in e-government against cyberattacks on adopted clouds.

Contents

List of Figures

List of Tables

List of Abbreviations

AI	Artificial Intelligence
API	Application Programming Interface
BCM	Business Continuity Management
BPMN	Business Process Model and Notation
BSI	Bundesamt für Sicherheit in der Informationstechnik
C5	Cloud Computing Compliance Criteria Catalogue
CASB	Cloud Access Security Broker
CIEM	Cloud Infrastructure Entitlement Management
CISO	Chief Information Security Officer
CPO	Cloud Product Owner
CSPM	Cloud Security Posture Management
DDoS	Distributed Denial of Service
DSGVO	Datenschutz-Grundverordnung
DSR	Design Science Research
DVC	Deutsche Verwaltungscloud
EU	European Union
EUCS	European Cloud Certification Scheme
FITKO	Föderale IT-Kooperation
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
GDPR	General Data Protection Regulation
HOU	Head of Organizational Unit
IaaS	Infrastructure as a Service
ICT	Information and Communication Technologies
IDS	Intrustion Detection System
ISMS	Information Security Management System
KPIs	Key Performance Indicators
LLM	Large Language Model
NIST	National Institute of Standards and Technology
OICD	OpenID Connect
OZG	Onlinezugangsgesetz
PaaS	Platform as a Service
PII	Personally Identifiable Information
RPA	Robotic Process Automation
SaaS	Software as a Service
SASE	Secure Access Service Edge
SCIM	System for Cross-domain Identity Management
SLAs	Service Level Agreements
SOC	Security Operations Center
ZenDiS	Zentrum für Digitale Souveränität der Öffentlichen Verwaltung

Part I

Dissertation Outline

1 Introduction

E-government encompasses the electronic processing of government data and the provision of digital services. The adoption of innovative information and communication technologies (ICT) in state and public institutions is intended to reorganise administrative processes more efficient, transparent and citizen-friendly [17]. In this context, administrative services are most frequently provided 24/7 via the Internet so that they can be used by citizens (G2C), enterprises (G2B) or other government organizations (G2G).

Web-based online forms allow the encrypted transmission of personally identifiable information (PII) as well as the secure electronic authentication of digital identities [25, 40]. For example, e-government makes it possible to submit tax documents [34], reserve a childcare place or register a new car from anywhere in the world. As a result, time-consuming on-site appointments at public offices are no longer necessary and the technical requirements are in place to process digitally recorded data in administrative systems without media discontinuity.

In practice, various ICT applications are used in parallel to support the multifaceted e-government processes, e.g. citizen portals, video conferencing solutions, secure file sharing tools, information systems for city councils, translation services or platforms for the dissemination of real-time data for smart city actors [16]. From a technical perspective, software solutions have long been hosted locally in data centers or software from government outsourcing partners have been used. For a few years now, powerful cloud services have increasingly been adopted in e-government as part of the digital transformation [16, 27].

Cloud Computing is a paradigm that has completely revolutionized the ICT industry, its technologies and business processes since 2010 and will continue to influence the relationships between providers, customers and end users in the future. The term describes the provision of IT resources via the Internet. Instead of operating software, computing power, storage space or other IT services locally on devices or servers, these resources can be obtained via the internet from cloud service providers [3]. The NIST defines cloud computing on the basis of three service models (SaaS, PaaS, and IaaS), four deployment models (private cloud, community cloud, public cloud, and hybrid cloud), and five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service) [44].

SaaS enables direct interaction with web-based applications directly via the browser on computers or smartphones, without the need for installation. Furthermore, software developers can use the libraries, databases and frameworks provided by the cloud service provider to design new cloud services with these platform tools (PaaS). With both service models, users generally have no control over the underlying infrastructure. By using IaaS, it is possible to administer virtualized servers or high-performance computing power engines in order to manage proprietary applications on these cloud resources.

This is made possible by the characteristics of cloud computing: Users can allocate IT resources such as computing power, storage space or network capacity directly as

required via an API or the web interface (on-demand self-service). Cloud services can be accessed from almost any device via an active internet connection (broad network access). Based on a multi-tenant architecture, cloud service providers are able to bundle physical and virtual resources and dynamically allocate them to different cloud users at the same time in order to utilize economies of scale (resource pooling). Due to the flexible configuration options of cloud services, it is possible to quickly scale them up or down to meet current business needs (rapid elasticity). The cloud services provided are monitored on an ongoing basis so that consumption-based payment is possible. In addition, the use of cloud services can be optimized through permanent recording of KPIs (measured service).

The focus of this dissertation is on the deployment model of public cloud services. Labes et al. published a taxonomy for deployment models of cloud services (see Figure 1) which covers both the cloud provider dimension and the cloud customer dimension [39]. As soon as one cloud service provider offers its services to several non-cooperating customers, it is known as a "public cloud service". Examples of public cloud services are in the context of IaaS (Amazon AWS, Google Compute Engine, Microsoft Azure Cloud, Oracle Cloud Infrastructure, etc.), PaaS (Atlassian Jira, Mendix Platform, SAP Build, ServiceNow App Engine Studio, etc.) or SaaS (DRACOON, Microsoft 365 Apps, Salesforce, etc.). In contrast, once cooperating customers or providers interact with each other, the deployment model becomes a "community cloud service". In the context of e-government, the cloud services offered are provided exclusively for authorities and public administrations by a government IT data center.

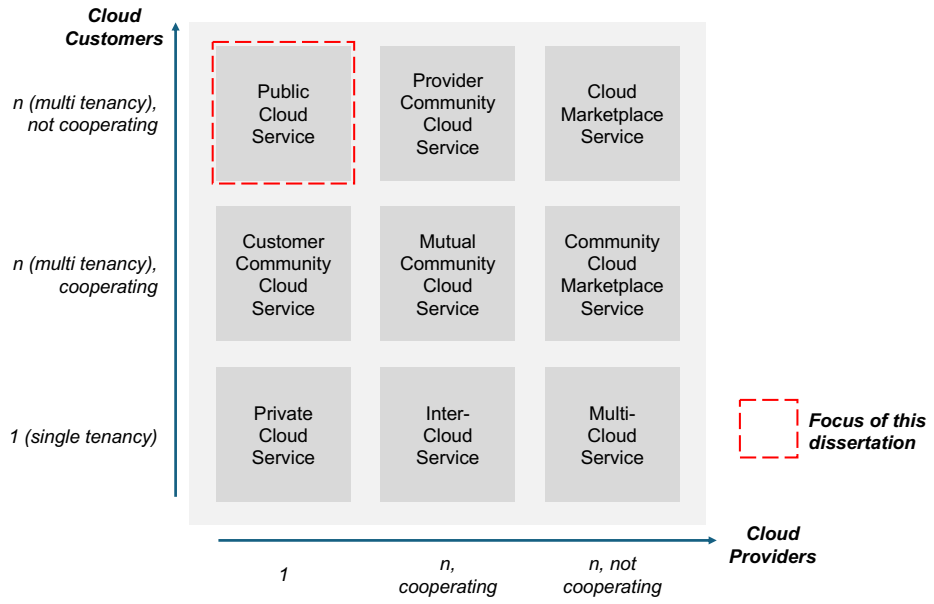


Figure 1: Classification of cloud deployment models (based on Labes et al., 2015)

1.1 Cloud opportunities, risks, and utilization

Opportunities: The adoption of public cloud services has several advantages for the e-government sector [4, 49, 44, 3]. The most important of these include cost efficiency and scalability, as expensive hardware investments and the associated maintenance costs are eliminated. Instead, cloud resources can be requested quickly and flexibly as required. This is particularly useful for e-government applications that have seasonal or unpredictable load peaks, e.g. mass events, unpredictable events. Furthermore, compared to on-premise systems, public cloud services enable a much faster provision of web-based services, as no time-consuming set-up processes for hardware and software are needed. This accelerates the digitalization of administrative processes. Cloud service providers also take on advanced security measures, e.g. DDoS and IDS protection, load balancing, enhanced SOC services, etc., depending on defined SLAs. Even more important for e-government is the opportunity to participate in technological innovations, e.g. AI applications, big data technologies or RPA solutions for the automation and optimization of administrative processes.

Risks: At the same time, there are also risks associated with the use of public cloud services. Because sensitive data or PII is no longer processed in local data centers, this data is entrusted to cloud service providers. As a result, this data is no longer fully under the control of the cloud customer. Public cloud services are accessible via the internet, which increases the risk of cyberattacks in connection with incomplete system configurations. Unauthorized parties could thus gain (unnoticed) access to sensitive data or PII of citizens, which not only violates information security but also data protection rights (cf. EU GDPR). Furthermore, dependency on cloud service providers increases, especially when using PaaS or SaaS solutions (vendor lock-in effect). An increase in license costs would result in unexpected additional costs. Due to the lock-in effect, a quick and easy migration to a more cost-effective cloud provider is time-consuming and cost-intensive due to the frequent lack of interoperability. Cloud customers are generally responsible for administering data, devices and user accounts. In particular, this requires the integration of cloud users into the organization's information security processes. There is a risk that a lack of knowledge among cloud administrators and incomplete security processes could jeopardize the operation of public cloud services. In addition, the applicable regulatory requirements must be observed when processing PII in public cloud services and each EU country has regulated the GDPR requirements in national law, e.g. DSGVO in Germany.

Cloud adoption in Germany: According to the KPMG Cloud Monitor 2021 [35], the use of cloud computing in the German economy developed rapidly between 2011 (28%) and 2021 (82%). In 2021, 46% of the companies surveyed used public clouds and 63% private clouds. Enterprise use of public clouds increased more than private clouds for the first time between 2019 and 2021. The Cloud Monitor 2023 [36] shows that more than 60% of companies plan to migrate more than half of their productive applications

to public clouds within the next three years. Security compliance services from public clouds are increasingly being used to improve information security.

Challenges of Cloud Computing in Public Administrations: There are numerous publications in research that examine the challenges and hurdles in the adoption of cloud services in eGovernment [31, 47]. David et al. [19] investigated the dimensions of people, processes and technology in their study based on a literature review in this area of conflict and identified the following causes: *People* (Lack of technical staff and knowledge, Lack of decision-makers' support, and Accelerate the inequalities in society), *Processes* (Lack of ethical framework and regulation, Lack of planning, and Lack of internal and external collaboration), and *Technology* (Lack of security and privacy, Lack of technical infrastructure readiness, Data-related challenges, and Compatibility).

On the other hand, public administrations were implicitly forced to use public cloud models for e-government. During the Covid-19 pandemic, digital solutions had to be implemented very quickly in order to reorganize administrative processes, e.g. making online appointments, online forms for administering vaccinations, etc. Regulatory requirements (e.g. Single Digital Gateway) are forcing authorities to improve their digital offering of administrative services [6]. In order to realize G2C, G2B, and G2G collaboration, new types of software programs are needed that have the corresponding interfaces integrated [26]. Overall, software is increasingly being offered as a SaaS solution, which is gradually replacing classic on-premises applications (e.g. Microsoft 365 etc.).

Due to the reluctance of public administrations to proactively address the secure operation of public clouds, they are now faced with a dilemma: office applications such as Microsoft Office 2016 and 2019 will no longer receive security updates from October 2025 and future identity and license management will increasingly be provided by Microsoft Entra ID[1]. In some cases, collaboration solutions can only be used through the integration of public cloud services, e.g. video conferencing. In the future, AI solutions (i.e. ChatGPT) will also be implemented as part of the digital transformation, making the interaction with LLM libraries in powerful public clouds unavoidable. The pressure from employees will increase on ICT departments to provide innovative products from external cloud services due to the associated shortage of ICT experts in public sector.

[1] https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id

1.2 Problem definition

Public administrations in Europe are facing huge challenges in implementing the urgently needed digital transformation [1, 2]. To make this a success, people, processes and technologies must be harmonized in the digitalization process. This requires ICT specialists who are able to analyze and optimize existing processes and are familiar with and can integrate the possibilities of ICT technologies.

However, according to a McKinsey study [43], there will be a shortage of 140,000 IT specialists in public administration in Germany by 2030 and a total of 1 million professionals according to a PwC study [50], making the digital transformation an even greater challenge. At the same time, existing ICT staff will have to provide operational support for existing software systems and integrate new legal requirements into the IT architecture. As a result, only limited human and financial resources are available for digital transformation in public administrations.

Public cloud services are a basic technology that can significantly support the digital transformation. SaaS solutions provide a fast and cost-effective approach of quickly and easily mapping processes digitally. However, the problem in the procurement process is that due to the lack of knowledge about cloud computing (see Subashini et al. [56]), important security features (e.g. identity management connectors) are not available in SaaS solutions, which means that these cloud services will have to be managed manually in the future.

Furthermore, the ICT departments of public administrations must be involved, as communication with public cloud services takes place directly via internet connections. This can be both an advantage and a disadvantage for digitization projects. Ultimately, the necessary expertise must be available at cloud customers so that data protection and security requirements can be implemented for this asset class.

Particularly in the context of the *division of responsibilities*, it becomes clear that the use of public cloud services is based on a *Cloud Shared Responsibility Model* [46] (cf. Amazon[2], Google[3], Microsoft[4]). In principle, responsibility for data, endpoint devices and user accounts lies with the cloud customer side (see Figure 2). However, the cloud customer needs to define the organizational units responsible for operating cloud security management tasks.

At the same time, it should be noted that cyberattacks on private and public organizations have increased significantly worldwide in recent years (cf. ENISA threat landscape 2023 [23], BSI State of Security in Germany 2023 [12]). Public administrations with e-government services are also severely affected by this, although security tools and frameworks for managing information security (e.g. ISO 27001 [28], BSI IT-Grundschutz Compendium [11], etc.) have long been established.

[2] https://aws.amazon.com/compliance/shared-responsibility-model
[3] https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate
[4] https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

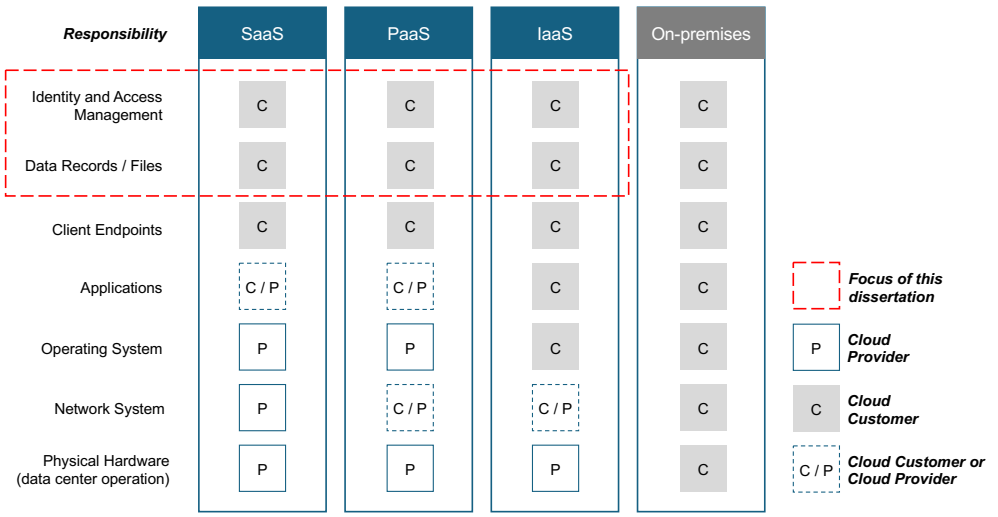


Figure 2: Cloud Shared Responsibility Model (based on NSA, 2024)

In Germany, cyberattacks on public authorities and local administrations are also increasing dramatically (cf. Kommunaler Notbetrieb[5], Konbriefing[6] Cyberangriffe auf die öffentliche Verwaltung). For example, the system failure of cloud provider SIT resulted in more than 125 cities having no access to their data for several months.

Overall, this leads to the following **problem specification**:

> Public cloud services are becoming increasingly indispensable in government institutions. At the same time, public administrations in Germany are struggling with a variety of challenges in the ICT sector. For this reason, there is a significant lack of research regarding the management of information security for public cloud services within public administrations.

The remainder of this dissertation is structured as follows. First, Section 2 provides a comprehensive overview of developments in the context of public cloud services in e-government and the most important EU research projects dealing with the information security of cloud computing. Based on this, the research questions of this dissertation are explained in Section 3. Section 4 describes the underlying research method, which provides the framework for processing the individual research contributions. The results of the individual research contributions are presented in Section 5. An overview of the publications produced in this dissertation is given before the main findings are described. Section 6 summarizes this dissertation and provides an outlook for future research. Part II contains the original scientific contributions.

[5] https://kommunaler-notbetrieb.de
[6] https://konbriefing.com/de-topics/cyber-angriffe-oeffentliche-verwaltung.html

2 Developments in Research and E-Government

During the course of this dissertation, numerous scientific contributions were identified that dealt with solving problems related to the management of information security of public cloud services in general. Germany has been actively involved in these research projects in recent years and has launched several initiatives since 2020 to establish secure and sovereign cloud services for public administrations.

Academic Research Projects on Cloud Security

In December 2023, the European Commission launched the research project IPCEI-CIS[7] (Next-Generation Cloud Infrastructure and Services) as part of the overall IPCEI strategy (Important Project of Common European Interest). The aim is to develop a "multi-provider cloud edge continuum" to strengthen data sovereignty in European countries [5]. There are currently 113 sub-projects registered in this research project, involving partners from research and industry from 12 EU countries, which are supporting the research project with up to 1.2 billion euros from public funds. Currently, 23 IPCEI-CIS sub-projects are already being carried out in Germany. The AIDED sub-project focuses on the secure and data protection-compliant application of AI solutions for the automation of recurring tasks in public administrations. IPCEI-CIS is also driving the development of a high-performance hyperscaler cloud infrastructure that will make both industry and public administration competitive.

IPCEI-CIS will partly build on the results of the Gaia-X project[8]. This aims to establish a secure and trustworthy data infrastructure for Europe [8]. In addition to European partners from research and industry, major US cloud providers are also involved in the development of Gaia-X.

In the EU research project MEDINA[9], artifacts like the specification of the Cloud Security Certification Language have been developed since 2020 for the continuous certification of cloud service providers. This is intended to increase the trustworthiness of public cloud services through compliance with the EUCS [22].

EU-SEC[10] was an EU research project between 2017 and 2019 in which a framework for a reference architecture (governance, risk management, security and compliance) was constructed to complement existing third-party attestations of cloud services. As part of EU-SEC and MEDINA, the Fraunhofer AISEC research group has developed the Clouditor[11] audit tool. This supports automated and continuous security checks in the public clouds of Amazon Web Services, Microsoft Azure or Kubernetes clouds by using cloud provider APIs. The aim is to check the actual cloud configurations against the compliance requirements from BSI C5 [10], EUCS [22] or CSA CMM [18] on the basis of machine-readable metrics.

[7] http://ipcei-cis.eu
[8] https://gaia-x.eu
[9] https://medina-project.eu/public-deliverables
[10] https://www.sec-cert.eu/eu-sec/deliverables
[11] https://www.aisec.fraunhofer.de/de/forschungsabteilungen/SAS/Clouditor.html

AUDITOR[12] is a research project funded by the Federal Ministry for Economic Affairs and Energy (2017 - 2024) with the aim of designing a data protection certification for cloud services that is sustainably applicable in accordance with Article 42 GDPR [52]. All actors involved in the process (cloud customer, cloud provider, end user, audit and certification body) are to be integrated. The legally reviewed data protection certification standard for cloud services (GDPR-CC), which has been approved since 2024, will be offered on the market in future by the Trusted Cloud[13] competence network. In addition, certified cloud services are listed on the Trusted Cloud website. At the same time, enormous efforts were made by this research group in another funded project in the area of regular dynamic certification of cloud services [41, 42, 55]. At the same time, the Value4Cloud research project (2011 - 2014) developed approaches to establish trust and legal compatibility for the use of cloud services. Among other things, a catalog of criteria for cloud provider selection was developed for this purpose [54].

PRISMACLOUD[14] was an EU research project (2015 - 2018) that promoted secure end-to-end communication between cloud users and cloud service providers using cryptographic concepts. The deliverables developed were evaluated in the application domains of Smart City, eHealth and eGovernment.

As part of the "Cloud for Europe" research project, research was carried out between 2013 and 2017 into how the utilization of cloud computing can simplify collaboration between public authorities and industry. One of the aims was to identify obstacles to cloud use. This project also aimed to research mechanisms for building trust in cloud computing systems [37].

Research on Cloud Security in Public Administrations

From 2010 to 2012, a few scientific studies were carried out by Fraunhofer that dealt with the use of cloud computing in public administration in Germany. It was already apparent in 2013 that Germany had a lot of catching up to do compared to other European countries [60, 59], but was able to close the gap over time [57].

There are no more up-to-date studies that focus on the use of public cloud services in eGovernment or public administration in Germany. A study on the use of cloud services in German authorities was conducted this year. However, the study [58] was not published until this dissertation was submitted. The preliminary results [45] show that only around 20% of administrations in Germany have implemented a cloud strategy. Very few of them have fully implemented the BSI's cloud security guidelines.

Furthermore, there is very limited research that has examined the adoption and use of cloud services in public administrations in other European countries, e.g. Norway [21], Portugal [7], Poland [15, 9], Sweden [26], United Kingdom [32], Greece [38].

[12] https://www.auditor-cert.de/en/publications
[13] https://www.trusted-cloud.de/dsgvo-zertifikat.html
[14] https://prismacloud.eu

Sovereign cloud services for public authorities in Germany

The industrial development of secure and sovereign cloud solutions for government organizations is highly dynamic. The market has now recognized that the cloud services offered to date cannot meet the requirements of public administrations. Enormous efforts have been made in Europe for several years to meet the requirements of government institutions with regard to data protection (e.g. GDPR, DSGVO, etc.) and to strengthen digital sovereignty (e.g. EU-US Data Privacy Framework, US CLOUD Act). The objective is to develop solutions for data protection-compliant, secure and sovereign cloud services for public administrations. Based on the aforementioned EU research projects and the resulting scientific findings, a large number of technological cloud solutions have now been developed to support public authorities in Germany in their digital transformation. In addition, Covid-19 and the implementation of the OZG in Germany have led to utilization of SaaS applications for e-government.

The "Deutsche Verwaltungscloud-Strategie"[15] (DVS) shapes the foundation for establishing the digital sovereignty of ICT in public administrations in Germany [33, 13]. The DVS takes into account the multi-cloud strategy pushed by the German federal government, which integrates open interfaces and common standards with high security requirements. In addition, special federal differences in Germany are to be taken into account in the development of cloud concepts. Since 2022, govdigital has been working on the prototype construction of a Cloud Service Portal[16]. This is to form the key component for the Deutsche Verwaltungscloud (DVC). FITKO is responsible for developing innovative cloud services and integrating them into the DVC[17]. The DVC is currently still in the development phase. The DVS plans to bundle federal, state and municipal cloud services, Gaia-X and external providers of public cloud services in the DVC. It is planned to connect different types of cloud service providers to the DVC.

Although many valuable outputs have been achieved in research over the last 10 years, these have so far only partially contributed to solving the problems described in public administration (see Section 1). Especially with regard to public cloud services that do not have an API for dynamic and continuous cloud certification, there are significant gaps in research on how these can be integrated into the processes of information security management in organizations. Doubrava et al. [20] put it in a nutshell: *"Cloud computing is the backbone of public administration in the implementation of digitization."*

In future, it will be much more important to talk about how the cloud can be securely integrated and used (security in the cloud) than to discuss cloud security in general (security of the cloud) [20]. Added to this are the rapid developments associated with the establishment of the DVC. For example, ZenDiS is developing the sovereign cloud platform openDesk[18].

[15] https://www.bmi.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html

[16] https://www.marktplatz.govdigital.de

[17] https://www.deutsche-verwaltungscloud.de

[18] https://www.opendesk.eu/de

3 Research Questions

The information security management of public cloud services in public administrations as e-government accelerator will be indispensable in the future. Moreover, public administrations are being forced by the digital transformation to implement public cloud services, i.e. AI platforms. These are not always provided by trustworthy government ICT providers. In view of the current situation, the identified problem definition (see Section 1) and the current developments in research and practice (see Section 2), the following main research question needs to be derived:

> ***How can public administrations in Germany operate IT services from public clouds securely and in compliance with data protection regulations?***

Due to the larger scope of this issue, it is divided into three central Research Fields: Cloud Security Management, Cloud Audits, and Cloud Utilization.

Research Field I: Cloud Security Management
Numerous methods, frameworks and technologies have been researched and are commercially available to increase information security in systems, applications and processes within organizations. While the industry has been dealing with information security for cloud computing for more than ten years, it has become omnipresent in government organizations in Europe at the latest since the Covid 19 pandemic. The aim of this dissertation is to explore pragmatic ways to make the utilization of public cloud services in public administrations more secure by focusing on the previously identified problems. For this purpose, the actors involved needs to be identified and the existing security concepts analyzed. In this regard, two research questions examine these aspects from two different perspectives:

> **RQ1**: *How can employees who are responsible for cloud services be involved into information security management processes?*

This research question focuses on the perspective of stakeholders in public administrations. The aim is to identify roles and organizational units that are responsible for the operation of public cloud services. Furthermore, the tasks and responsibilities of the identified stakeholders will be determined. Of central importance here is how organizational changes (e.g. departures, changes of affiliation) in local authorities can be integrated into cloud security management processes.

> **RQ2**: *How can security processes for public cloud services in public administrations be improved?*

Due to the large number of areas of responsibilities within public administrations, it is highly likely that several public cloud services are operated decentrally. However, it is the responsibility of CISOs to maintain an overview of the cloud services in use. Based

on this research question, this dissertation analyzes how public cloud services adopted in public administrations can be integrated into information security management processes. In this context, it is examined how this can be realized if public cloud services do not offer APIs for audits.

Research Field II: Cloud Audits
Security audits carry out systematic reviews and assessments of the security requirements in information systems in order to identify weaknesses and potential for improvement. Any deviations identified must be systematically monitored so that a higher level of information security maturity can be achieved. This leads to the following research question:

> **RQ3**: *What criteria and aspects must cloud audits include so that public administrations can build the necessary trust in the information security of public cloud services?*

Two practical problems are to be addressed by answering this research question. The first is to empirically investigate which cloud certifications exist on the market and how they differ from one another in terms of content. The aim is to examine the extent to which these are suitable for the application in public administrations. Secondly, research will be conducted into how those responsible in public administrations can independently check public cloud services with regard to standardized security requirements. In this context, the interaction between people, persons and technologies will also be evaluated.

Research Field III: Cloud Utilization
In order to gain a better practical understanding of the problem identified, a comprehensive exploration of the utilization of cloud services in public administration is required. In this context, the focus is on two research questions:

> **RQ4**: *To what extent are public cloud services already being used in German authorities and for what purposes?*

The aim is to investigate how intensively cloud computing is used in the public sector, as the studies available on the market only take minimal account of this domain. In this context, it is important to determine the application purposes for which public clouds are used.

> **RQ5**: *What security concepts exist in German authorities to ensure data protection and information security of used public cloud services?*

This analysis is intended to investigate how public cloud services in public administrations are currently integrated into information security management processes. In this context, the focus is particularly on the security requirements from the BSI IT-Grundschutz for cloud usage.

4 Methodology

In order to address the research questions RQ1 - RQ5, it is necessary to consider several factors in this research field together. The introduction of new technologies in organizations inevitably leads to changes in terms of people, processes, structures and culture [30]. The adoption of public cloud services in public administrations has resulted in a paradigm shift. This has an impact on established *processes*, long-standing organizational *structures*, the *culture* of collaboration, and *employees*. However, these factors must be interlinked in the holistic management process of information security [53].

In this dissertation, two different research methods are used to generate new knowledge in order to answer the research questions [29]. To answer RQ1, RQ2 and RQ3, the *design science research* methodology of Hevner et al. is used [24]. This promotes a design-oriented research approach in information systems research. To answer RQ4 and RQ5, the application of a *quantitative research* methodology is required.

Design Science Research

DSR is a design-oriented research approach that promotes the construction and evaluation of artifacts to solve specific real-world problems. Peffers et al. [48] have developed a methodology for DSR that, starting from a practical problem, forces the development, demonstration and evaluation of artifacts, including the publication of the results (see Figure 3).

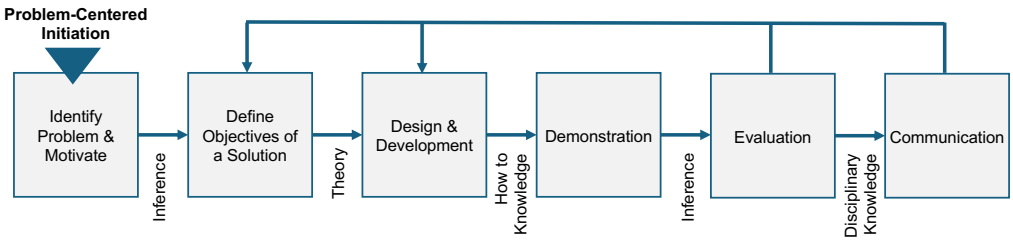


Figure 3: Process model for the DSR methodology (based on Peffers et al., 2007)

In DSR projects, the guidelines according to Hevner et al. [24] must be observed so that scientific findings are generated in addition to practical contributions. The DSR cylce contains rigorous and relevant approaches.

- **Guideline 1: Design as an Artifact**: DSR focuses on the creation of new artifacts, e.g. technological tools, models, methods or instances. The aim is to solve specific problems or to achieve an improvement. To fulfill this guideline, tool-based artifacts are designed in this dissertation in papers P1, P4, and P5 (see Section 5).
- **Guideline 2: Problem Relevance**: DSR is a scientific method designed to solve practical problems. This practical problem has been precisely described in Section 1. It concerns the management of information security of public cloud services in the public sector.

- **Guideline 3: Design Evaluation**: The rigorous evaluation of the developed artifacts is a central component of DSR. The evaluation can be carried out using various approaches, e.g. tests, case studies, etc. In this dissertation, the developed artifacts are tested in a concrete problem space with employees based on practical use cases.
- **Guideline 4: Research Contributions**: DSR aims to generate new knowledge for research. This knowledge can result in the form of new theories, models or methods so that they can be applied to different problems or contexts. The outputs of papers P1, P4 and P5 provide generally applicable methodological approaches on how the use of tools can improve the management of information security of public cloud services in public administration.
- **Guideline 5: Research Rigor**: Scientific rigor must be included in the construction of the artifacts and in their evaluation. The tools developed in this dissertation are based on existing scientific results, e.g. graphical visualizations.
- **Guideline 6: Design as a Search**: The design process is considered to be an iterative search for different solutions and approaches in order to promote the best possible approaches for the construction of the respective artifact. When working on the research questions in the DSR process, alternative approaches were regularly sought in order to contribute to a solution to the problem.
- **Guideline 7: Communication of Research**: The outputs generated during the DSR cycle must be communicated to technical target groups such as researchers and developers, as well as to management and end users. The artifacts and practical solutions developed in this work have been published at scientific conferences (cf. Table 1) and presented to the professional audience.

Quantitative Research

To answer RQ4 and RQ5, the conduction of an online survey as a research method of quantitative research methodologies [29] is enforced. This offers the opportunity to comprehensively carry out the aspects associated with the research questions in a detailed and structured approach. The results of Paper P6 are based on a comprehensive online survey for which the *web survey process* according to Callegaro et al. [14] was applied (see Figure 4).

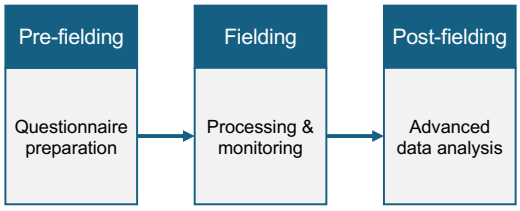


Figure 4: Generalized web survey process (based on Callegaro et al., 2015)

5 Results

The research contributions resulting from this cumulative dissertation are introduced in this section. First, an overview of the scientific articles and a classification to their research fields is provided below.

5.1 Overview of Research Papers

Based on the previously defined research questions (Section 3) and the applied research method (Section 4), a total of 6 scientific papers have been written. Each paper can be assigned to one of the three research fields to answer one or more research questions. Figure 5 provides an overview of the contributions in each research field.

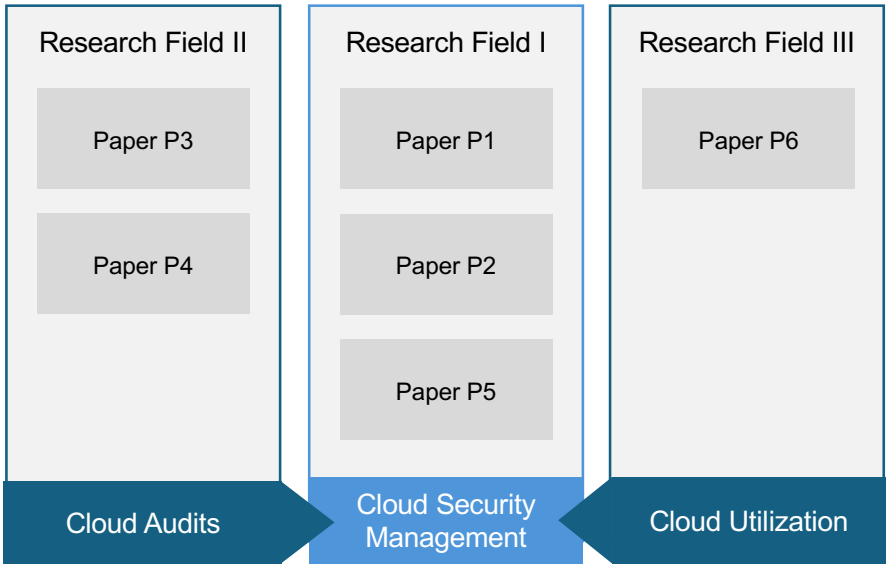


Figure 5: Overview of Research Articles and the associated Research Fields.

Table 1 lists the individual contributions chronologically according to their publication history. A total of four articles have been published at peer-reviewed conferences (C) in the field of computer science. One further paper has been submitted to a peer-reviewed journal (J). Furthermore, a contribution was written in the context of this dissertation in the research field of cloud security management, which was published in modified form as a guest contribution in a book (B) after several reviews.

The original article P3 was rejected by the Journal Problems and Perspectives in Management. After the disputation took place, the article has been revised, resubmitted, and finally published by the Journal Current Issues of Business and Law.

Similarly, the original article P6 was rejected by the Journal Public Money & Management. After the disputation took place, the article has been revised, resubmitted, and finally accepted at the ICISSP 2026 conference.

No.	Publication	Type	State
P1	DIENER, M., BLESSING, L., 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 Intern. Conf. on Availability, Reliability and Security (ARES)*, Salzburg, Austria, pp. 776-785.	C	published
P2	DIENER, M. (2022). Herausforderungen für öffentliche Verwaltungen im Zeitalter der Digitalisierung: ein kritischer Blick auf die Relevanz der Informationssicherheit. Guest contribution in section 8.2 within book: *Auf dem Weg zur digitalen Verwaltung : Ein ganzheitliches Konzept für eine gelingende Digitalisierung in der öffentlichen Verwaltung*, Springer, pp. 208-223.	B	published
P3	DIENER, M., ROESSLE, F., (2025). Cloud certification to foster digital transformation management in public administrations. In *Journal Current Issues of Business and Law (CIBL)*, pp. 30-47.	J	published
P4	DIENER, M., 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 Intern. Conf. on Information Systems Security and Privacy (ICISSP)*, Lisbon, Portugal, pp. 543-551.	C	published
P5	DIENER, M., BOLZ, T. (2024). Visualizing the Information Security Maturity Level of Public Cloud Services Used by Public Administrations. In *Proc. of the 14th Intern. Conf. on Cloud Computing and Service Sciences (CLOSER)*, Angers, France, pp. 192-203.	C	published
P6	DIENER, M., MEUCHE, T. (2026). Utilising cloud services in local governments as digital transformation booster by mastering information security duties. In *Proc. of the 12th Intern. Conf. on Information Systems Security and Privacy (ICISSP)*, Marbella, Spain, pp. 565-576.	C	accepted

Table 1: Overview of research publications.

Research Field I, the central component of this dissertation, focuses on cloud security management. Three publications are assigned to this research field. In a first step, the adoption of file sharing services from public clouds was investigated (Paper P1). This

paper uses machine learning to generate suggestions for public clouds, depending on the sensitivity of the document content. After focusing the research questions on the public sector, the existing challenges of information security management of public cloud services in public administrations were examined and addressed in a scientific book contribution (Paper P2). In addition, the tool-based prototype has been optimized with the knowledge gained in order to support the actors involved in public administrations. The aim is to improve the management of security requirements for decentrally managed public cloud services with graphical visualizations (Paper P5).

Research Field II addresses the auditing of cloud services in public administrations. Paper P3 compares the certifications of cloud services available on the market. The results are used to discuss why the application of existing cloud certificates in public administrations is currently a challenge. In addition, a web-based prototype has been developed in this research field to carry out continuous security audits of public cloud services that do not have technical APIs and therefore do not allow automated checks (Paper P4).

In *Research Field III* a comprehensive empirical study is being conducted to determine the status quo of information security and the implementation of public cloud services in German municipal administrations (Paper P6).

5.2 Research Field I: Cloud Security Management

Research Field I looks at the organizational and technical challenges to ensure that public cloud services in e-government areas are operated more securely in the future. Compliance with the data protection regulations is also closely linked to this topic. The BSI IT-Grundschutz Compendium [11] is used as a reference, which sets out specific requirements for information security when using public cloud services.

Starting from the adoption of cloud services [P1], the basic tasks and problems for CISOs in public administrations are identified [P2]. Based on this, a technical prototype is developed that combines the three dimensions of people, processes and technology in order to establish the management of information security for this asset class in public administrations [P5]. With regard to the cloud lifecycle [51], the technical contributions in [P1] and [P5] provide valuable scientific input to ensure the adoption and operation of public cloud services.

[P1]: Tackling the cloud adoption dilemma - A user centric concept to control cloud migration processes by using machine learning technologies

When the first public cloud services became available on the market, many companies were initially reluctant to adopt them. Instead, the focus was on the integration of private cloud solutions. Numerous studies primarily identified concerns regarding information security and data protection. Challenges in terms of adhering to compliance requirements were also mentioned. Public administrations had no interest in cloud technologies at that time, as internal ICT resources were sufficient for processing PII. At the same time,

companies recognized that the services offered by public clouds could be helpful and economical. The result was a dilemma regarding the adoption and integration of public cloud services into local IT architectures. In general, the basic problem was based on the lack of trust of cloud customers in cloud products. For this reason, research efforts were made to develop cloud adoption frameworks and encryption techniques for data within cloud infrastructures. This paper refers to **RQ1** and examines how employees in organizations can be involved in cloud security processes to protect PII data.

The idea of this research project was to provide organizations with technical support for data migrations to public cloud file sharing portals using a tool. For this purpose, a logical connection was built between the documents to be migrated and public cloud services that are compliant. The documents are assigned to specific document categories depending on their content. Each document category is assigned to a protection requirement class. Depending on the protection requirement class, public cloud services that are permitted to process such content are released. A machine learning approach based on a Naive Bayes classifier was used to assign document content to document categories. A supervised learning approach is applied to generate the machine learning model. For this purpose, a prototype application based on Java was programmed (see Figure 6) which contains three components: Document Inspector, Model Trainer, and Policy Manager.

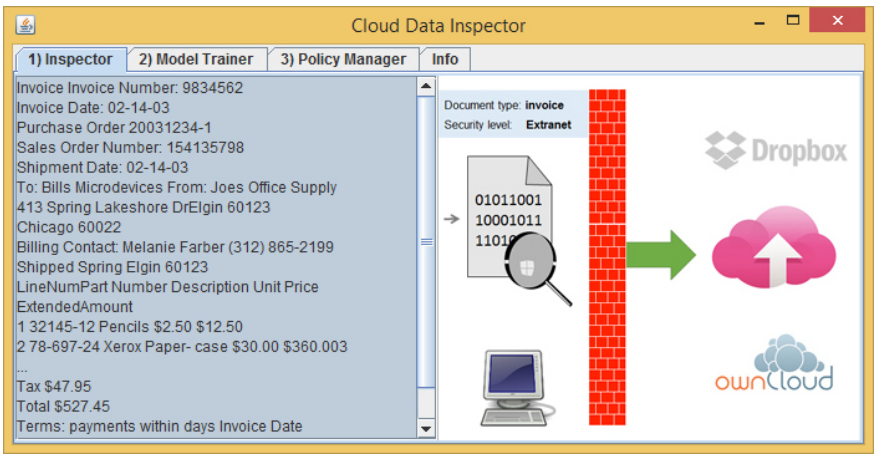


Figure 6: Document analysis with the Cloud Data Inspector.

The logical connection between document category, protection requirement class and public cloud service is formalized with the *Policy Manager*. The Model Trainer is used to train the machine learning model. For this purpose, the contents of documents are extracted into plain text with the help of Apache Tika. This technique is also used when inspecting documents that are to be migrated to a public cloud. As soon as the Naive Bayes Classifier within the *Document Inspector* has determined the document category, the Policy Manager can be applied to determine which of the predefined public cloud services may be used for the migration. Documents with critical content are not allowed to be migrated. Three platforms were considered as predefined cloud services: DropBox (low protection class), MagentaCloud (medium protection class) and OwnCloud (high protection class).

The proposed *Cloud Data Inspector* was evaluated as part of a laboratory study. A total of ten participants successfully tested the tool. They tested the functionality of the tool with various documents. The contents of the documents were changed manually by the participants to test the correct assignment of suitable public cloud services using the prototype. Eight out of ten participants confirmed that using this prototype increased their availability to utilize external file sharing services. However, the speed of the tool slowed down rapidly the larger the trained machine learning model was.

Contribution: The secure use of public cloud services in organizations can be increased if security tools support the cloud migration process by providing dynamic security policies based on data categories, among other things. Due to the enormous amounts of data that are regularly processed in public administrations, tool support (e.g. data loss prevention) appears to make sense in multi-cloud architectures. For example, the approach presented can be used to influence the selection of the storage location of data in cloud-based working spaces depending on their protection requirements, e.g. apps in Microsoft 365, public cloud services within the DVC, etc. At the same time, it became clear in this research work that powerful machine learning algorithms are required to technically implement the classification of large amounts of data in local data centers.

[P2]: Herausforderungen für öffentliche Verwaltungen im Zeitalter von Cloud-, E-Government- und Smart-City-Projekten: ein kritischer Blick auf die Relevanz der Informationssicherheit

Public administrations in Germany are facing major challenges in connection with the digital transformation. The number of ICT applications used and their complexity is regularly increasing, as a wide variety of tasks have to be mapped using software as a result of legal requirements. This leads to a highly networked ICT architecture that is increasingly more dependent on external cloud services. For this reason, a wide variety of systems are being implemented in the DVC infrastructure in Germany so that innovative applications are available to public administrations. However, it is also clear that the tasks relating to the management of information security are also changing considerably as a result. In future, public cloud services will have to be considered differently and more intensively in the security processes of public administrations than was previously the case with local ICT systems. Therefore, the security requirements for the use of cloud services (cf. OPS.2.2 Cloud Usage [11]) will play a greater role in public administrations (see Figure 7).

In this publication, relevant research and practical contributions in the field of information security in public administrations have been compiled on the basis of a simple literature review to address **RQ2**. Based on this research question, the most important areas of information security are identified, which must be given even greater consideration in future e-government security concepts.

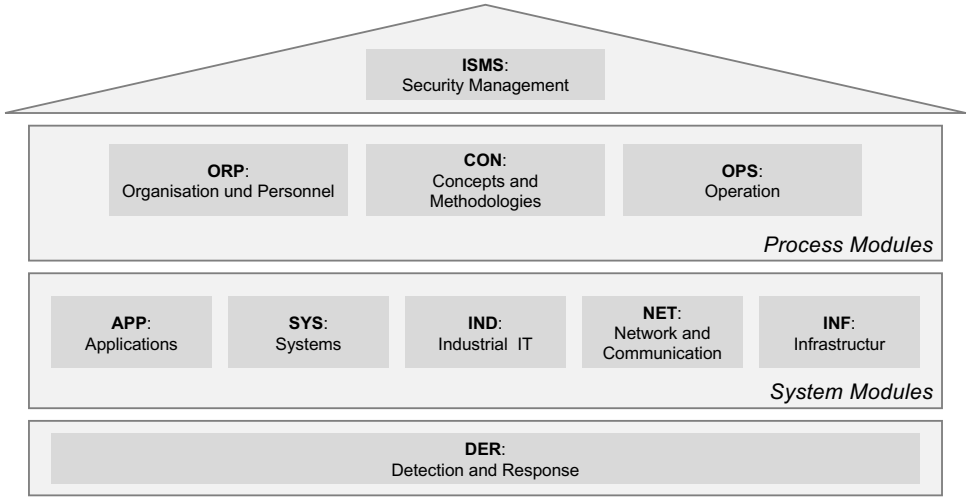


Figure 7: Layer model of BSI IT-Grundschutz (based on BSI-Standard 200-2).

The aim of this research paper is to present the changes and the associated challenges of information security issues in public administrations in Germany in a structured manner. The article is directed at managers and decision-makers in public administrations in Germany, who are increasingly having to deal with the effects of cloud computing in the context of AI and smart city projects. When identifying the publications, the established libraries ACM, dblp, IEEE and Google Scholar were searched for the search terms *[+"Public Cloud" +Informationssicherheit +Management AND ("öffentliche Verwaltung" OR Behörde OR Kommunalverwaltung)]*.

However, the number of existing German-language publications is very limited, although there is a considerable need for research in this application domain with regard to the problem definition (see Section 1).

Contribution: This article addresses essential tasks in the management of information security in public administrations. Against the backdrop of an increasing number of successful cyberattacks on German authorities, the establishment of an ISMS for secure e-government services is essential. The existence of a cloud strategy and up-to-date cloud documentation is an essential prerequisite for implementing suitable technical and organizational measures. Above all, the proactive integration of employees into information security processes is absolutely essential. Furthermore, the risks associated with the use of public cloud services must be increasingly taken into account in the future, as it is highly likely that PII will be processed outside the local ICT systems, e.g. AI Web Services. This research paper provides a structured overview of the responsibilities to be regulated, which are a mandatory prerequisite for information security and data protection in the decentralized utilization of public cloud services in public administrations.

[P5]: Visualizing the Information Security Maturity Level of Public Cloud Services Used by Public Administrations

Due to the situation in public administrations in Germany described in Section 2 and Paper P2, even more clouds will be implemented in the future. These are not always procured directly by ICT departments, but in decentralized departments with possibly less knowledge of cloud security. In this respect, different risks arise in public authorities that threaten the security and data protection of e-government processes. As a result, there is a lack of central overviews of the status quo of the adopted public cloud services. As a result, cloud audits are difficult to monitor. In addition, managers of public cloud services no longer perform (ad-hoc) administration due to departmental changes or departures, resulting in serious weaknesses in organizational security processes. Another problem is that many SaaS applications often have no APIs for identity management, e.g. OICD or SCIM, which means that external identity silos are growing rapidly. In addition, automated and continuous checks of cloud metrics (cf. Lins et al. [41]) are therefore not technically possible, meaning that the use of innovative concepts such as CASB, CSPM or CIEM is only possible to a limited extent or not at all.

Answering **RQ1** and **RQ2** from the practical perspective of a public authority, a prototype was designed based on the design science research method [48]. The developed tool supports CISOs in public administrations in maintaining an overview of adopted public cloud services and at the same time being able to monitor the progress of cloud security audits. For this project, several interviews were conducted with CISOs from other local authorities in Germany. This made it possible to identify approaches that can improve the management of information security for public cloud services. By applying this research method, it was possible to identify three central roles in public administrations that are regularly involved in the administration of public cloud services: CISO, HOU in whose department the public cloud service is operated, and at least one CPO who is responsible for user administration. Furthermore, three essential tool requirements that are important for tool support were identified by expert interviews:

- presentation of departments that use public cloud services
- status quo of running cloud audits
- status quo of cloud security measures

In a first step, a process model was developed based on the findings, which supports cloud audits with tool assistance for three phases (Inventorying adopted clouds, Auditing cloud security, Evaluating maturity level of cloud security). The developed process model (see Figure 8) in BPMN notation takes into account the three identified roles (CISO, HOU, and CPO) within e-government environments.

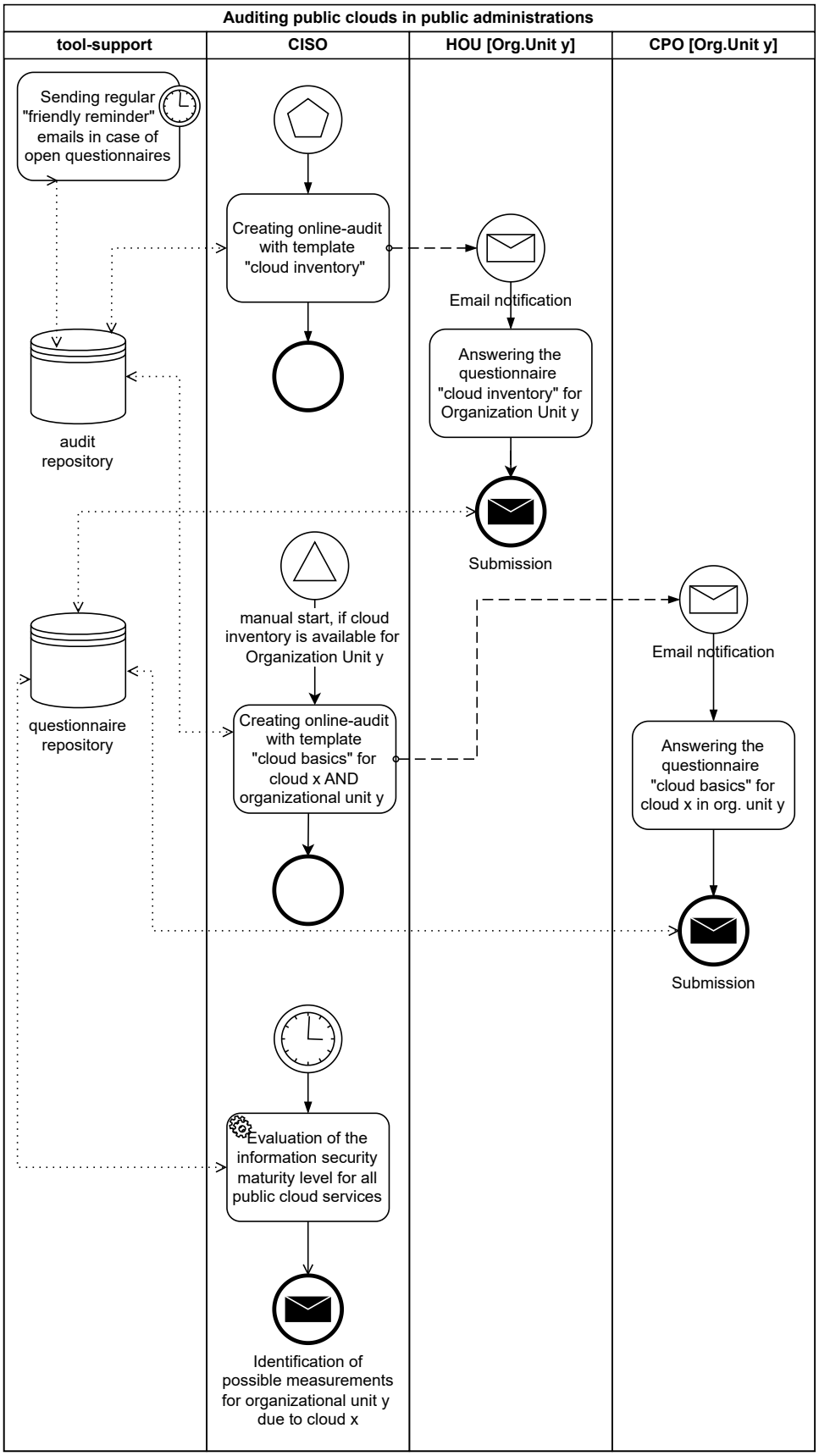


Figure 8: BPMN process model for cloud security audits related to public cloud services.

During the application of the DSR lifecycle process, several existing ISMS tools were also examined. However, it was found that they were unable to meet the identified tool requirements. Therefore, additional functionalities were added to the developed Cloud Inspector. As a result, it was possible to carry out cloud audits as well as to enable cloud security management for CISOs. In summary, the tool can assist employees in public administrations to improve the expected information security maturity level for adopted public cloud services by using realtime cloud dashboards. The dashboard can highlight anomalies (see figure 9) in the Organizational Units Assets Grid (OAG).

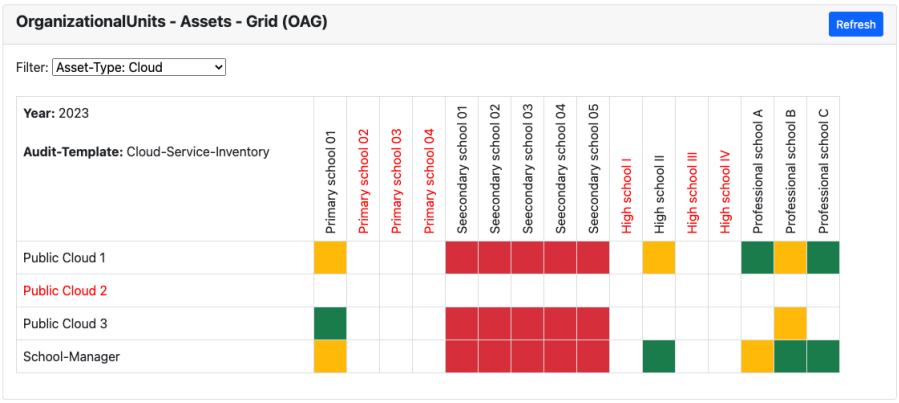


Figure 9: Visualizing correlations between OUs and public cloud services (OAG).

With this approach, cloud security management can immediately determine the status quo of cloud audits in relation to an Organizational Unit (OU) that have adopted one or more public cloud services. Furthermore, this visualization can be used to immediately identify which OUs are not using any clouds and which identified public cloud services are not currently being used by any OU. This visualization represents the central cockpit for the initiation of necessary cloud audits. Another visualization component, the Cloud Security Requirements Grid (SRG), was developed in this research work to monitor the individual cloud audits (see Figure 10).

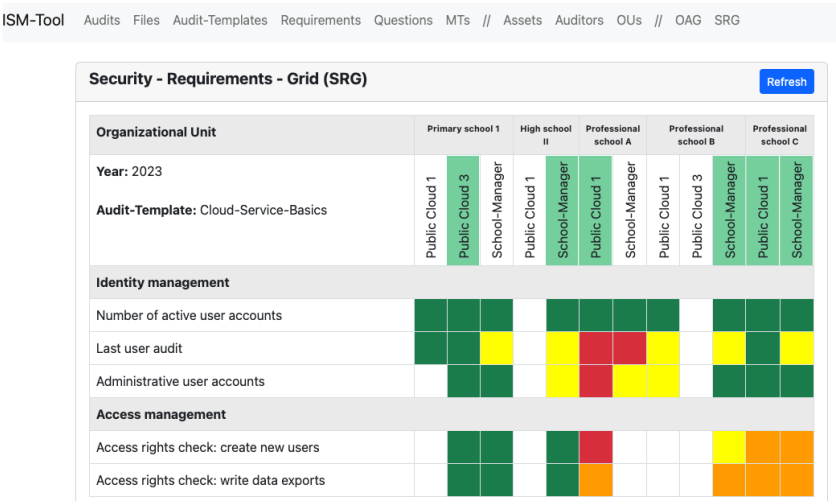


Figure 10: Overview of information security maturity level of public clouds (SRG).

This SRG dashboard provides CISOs with a clear overview of the cloud security requirements of the public cloud services in operation. The different colors in the visualization make it immediately recognizable which clouds in the departments of a public administration have a lack of security requirements. One disadvantage of these developed and evaluated prototype approaches is that the human factor always plays a role. This means that you have to rely on truthful answers from CPOs.

Contribution: The cloud security of public cloud services must be checked regularly, regardless of whether an API is available for audit checks. The persons responsible for identity management in such clouds must always be involved in the holistic security process of cloud security management. A public cloud must not be operated in a public authority without an active "cloud manager". At the same time, this research shows that innovative security tools are needed to support CISOs obtaining an overview of the status quo of ongoing information security processes. This is the only way to systematically identify potential vulnerabilities in external cloud resources at an early stage. The larger a public administration is, the higher the probability that different types of public cloud services will be used decentrally. This research paper has shown that enormous progress can be made in the area of cloud security management with simple visualizations.

5.3 Research Field II: Cloud Audits

To establish a holistic cloud security management system, both technical and organizational cloud audits must be carried out. Cloud audits are used to check predefined requirements from security frameworks. The results of cloud audits provide information on the degree to which and how comprehensively the expected security measures have been implemented. In Research Field II, the topic of cloud audits is examined in two scientific papers. First, certificates for cloud services are analyzed and evaluated for their suitability in public administrations [P3]. Building on this, it is shown how cloud audits can be carried out in public administrations with the help of innovative tools [P4]. This is particularly relevant for the public cloud services used, if they do not provide APIs for automated security checks.

[P3]: Cloud certification to foster digital transformation management in public administrations

The idea of cloud certificates is to verify compliance with defined data protection and security requirements in cloud services. A cloud certificate therefore serves as proof that the requirements are fulfilled or that there are only a few deviations. Various cloud certificates have existed on the market for several years. The BSI C5 Standard [10] developed in Germany certifies compliance with the highest security requirements, but has so far often only been applied to the cloud services of large hyperscalers. One of the reasons for this is that such cloud certifications are very expensive.

This scientific publication documents the results of a comprehensive literature review of existing cloud certifications for providing answers to **RQ3**. On the basis of predefined criteria, the most important certificates that consider the information security and data protection of cloud services have been identified. A total of 11 cloud certificates (see Table 2) were analyzed.

Certificate name	Provider	Provider organization type	Launch	Last Update	Main Focus	Type
AUDITOR	Auditor Cert	Government supported	2019	Jan 20	DP	Criteria Catalogue
BSI C5	BSI	Government	2016	Feb 20	IS	National Standard (Germany)
BSI IT-Grundschutz	BSI	Government	1994	Feb 22	IS	National Standard (Germany)
CSA STAR	CSA	Non-profit	2010	Jul 21	DP, IS	Criteria Catalogue
EuroCloud StarAudit	EuroCloud	Non-profit	2009	Dez 20	DP, IS	Criteria Catalogue
European Privacy Seal	EuroPriSe	Private	2007	Jan 17	DP, IS	Criteria Catalogue
ISO 27001	ISO	International association	2005	Sep 13	IS	International Standard
ISO 27017	ISO	International association	2015	Dez 15	IS	International Standard
ISO 27018	ISO	International association	2014	Jan 19	DP	International Standard
ISO 27701	ISO	International association	2019	Aug 19	DP	International Standard
Ö-Cloud-Gütesiegel	EuroCloud Austria	Non-profit	2021	Dez 20	DP, IS	Criteria Catalogue

Table 2: Summary statistics of cloud certificates.

On the basis of expert interviews, 8 criteria were determined, which were used to examine the identified cloud certificates in terms of their characteristics (see Table 3). The evaluation showed a very heterogeneous picture. Overall, the features *Management of Information Security*, *Risk Management* and *Business Continuity Management* are present in all cloud certificates. The *Official investigation information process* criterion differs considerably between the should-have and must-have features of the cloud certificates examined. The *Prevention of foreign state access* feature is not a must-have criterion for any of the 11 cloud certificates.

The ISO 27000 certification family is often cited as a requirement in public tenders. However, this is not sufficient to be able to make reliable statements as to whether a SaaS or PaaS application is actually secure and data protection-friendly. Rather, the data centers in which these are operated are certified with it. In this respect, the informative value of ISO certificates in the context of public cloud services is only of limited use to CISOs.

Another problem is that there is currently no central repository that lists the cloud services that have a valid BSI C5 certificate. In addition, all major US hyperscalers now have a BSI C5 certificate, although the *prevention of foreign state access* criterion is not included as a must-have requirement in this certificate as well. This means that the use of innovative cloud services from US hyperscalers in public administrations in Europe should still be viewed critically, despite BSI C5 cloud certification.

Certificate name	ISM	RM	BCM	Sub service provider documentation	Geo location documentation	Official investigation information process	Prevention of foreign state access
AUDITOR	✓✓	✓✓	✓	✓✓	✓✓	✓✓	x
BSI C5	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓
BSI IT-Grundschutz	✓✓	✓✓	✓✓	✓✓	✓	x	x
CSA STAR	✓✓	✓✓	✓✓	✓✓	✓✓	✓	x
EuroCloud StarAudit	✓✓	✓✓	✓✓	✓✓	✓✓	✓	x
European Privacy Seal	✓✓	✓✓	✓	✓✓	✓✓	✓✓	✓
ISO 27001	✓✓	✓✓	✓✓	✓✓	✓	x	x
ISO 27017	✓✓	✓	✓	✓	✓	✓	x
ISO 27018	✓✓	✓	✓	✓	✓	✓	✓
ISO 27701	✓✓	✓✓	✓✓	✓	✓	✓	✓
Ö-Cloud-Gütesiegel	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	x

Table 3: Cloud certificates fulfillment grade for public administration requirements.

The Cloud Security Alliance (CSA) registry[19] includes many CSA STAR Level 2 (third-party audit) certified cloud services from third countries (e.g. Australia, China). There is currently no Data Protection Agreement (DPA) for these countries in the EU. This means that although such cloud services are certified, they are not compliant for the use by public administrations in Europe due to the GDPR regulations.

In this scientific paper, a proposal based on EUCS [22] is discussed that combines the approaches of the US FedRAMP solution with a trusted marketplace for cloud services[20]. A closer look at the 494 certified cloud services in the FedRAMP marketplace reveals that only very few European public cloud services were able to meet the auditing standards, e.g. SAP Concur Cloud for Public Sector.

Contribution: The results show that various cloud certifications currently exist. The concerns of European authorities regarding data protection and security issues are currently not fully resolved by cloud certificates. There is currently no guarantee that prevention of foreign state access is fully guaranteed by the certified cloud service providers. Further developments regarding EUCS must be awaited, as it has not yet been released due to further sovereignty requirements. EUCS (cybersecurity) in combination with the AUDITOR certificate (data protection requirements) for public cloud services could be a promising solution for government organizations for comprehensive guarantees of compliance with legal requirements. However, this requires monitored cloud marketplaces (e.g. DVC marketplace) analogous to FedRAMP, in which only valid cloud certificates for public authorities are offered. Until then, public administrations in Europe will only be able to critically self-assess their planned or already deployed public cloud services.

[19] https://cloudsecurityalliance.org/star/registry
[20] https://marketplace.fedramp.gov/products

[P4]: Cloud Inspector: A tool-based approach for public administrations to establish information security processes towards public clouds

This research work tackles **RQ3** and **RQ1** from the perspective of CISOs working in public administrations. Practical observations during the course of this dissertation have shown that more and more public cloud services are being adopted decentrally by various organizational units in public administrations. The reason for this is that specific software applications are required in the departments. These cloud services generally do not have APIs, which means that continuous monitoring using [55] metrics is technically impossible. Cloud certificates cannot provide any insight into how secure a cloud is, as it depends on the individual cloud configurations and the processes between the cloud and the cloud customer's personnel who administer the system. A lack of awareness of information security among the cloud users who originally procured these public clouds was also identified. It is additionally problematic that existing ISMS tools do not currently contain any easy-to-use features that enable manual cloud audits to be carried out efficiently in decentralized organizational structures.

By applying the Action Design Research methodology, innovative ideas and concepts for the construction of an audit tool (Cloud Inspector) have been developed with experts from public administrations. The aim of the output of this scientific contribution is to develop a tool approach that can be used to check the status quo of the information security of public cloud services. In this context, it has become clear that the first step is to define a CPO for each public cloud service. These usually have no expert knowledge of cloud security, which means that many technical correlations must be implicitly explained in a cloud audit before it is possible to answer the questions about the examined cloud services. Another identified requirement is that such surveys must not take a long time. As a result, a methodical approach is needed that is self-explanatory. Both CISOs and CPOs have the requirement to avoid free text answers wherever it is possible. Due to the diversity of public cloud services and the requirement to audit them regularly, an automated evaluation of the security questions is absolutely essential.

In this article, a web-based tool has been developed to support the systematic implementation of cloud audits with CPOs. Among other things, the online questionnaire contains references to the security requirements from the BSI IT-Grundschutz compendium. The CPOs are presented with questions with predefined answer options. The answer options have assigned *sentiment* (positive, neutral, negative, unknown, remarkable), so that an automated and efficient evaluation of several cloud audits is possible (see Figure 11).

The constructed tool was comprehensively evaluated with regard to the derived feature optimizations. The evaluation of the practical suitability of the Cloud Inspector was carried out in a public administration under real conditions. The formalized security requirements of "ORP.4.A3 Documentation of User IDs and Rights Profiles" were checked using the example of productively operated public cloud services. Various CPOs had to answer an online questionnaire with the Cloud Inspector in relation to the public cloud

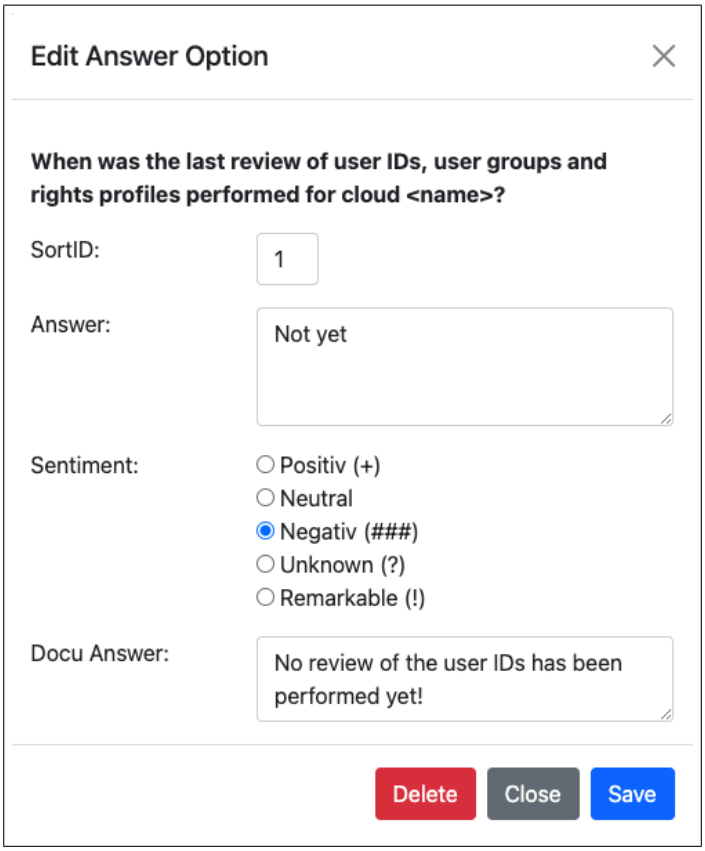


Figure 11: Specification of an answer option sentiment that is related to one question.

services they manage. The tool was continuously optimized and is now applied as a tool support for cloud audits in the holistic security process.

Contribution: This work showed that the procurement and implementation of cloud services in public administrations is often different compared to traditional IT projects. Clear rules are needed as to which security tasks the respective responsible parties must fulfill in the security process. This research paper shows that public cloud services can be subjected to continuous cloud audits without an API, provided that CPOs and CISOs are supplied with intuitive security tools. This includes web-based questionnaires that are simple and not time-consuming to complete. It must also be possible to automatically evaluate the responses received so that CISOs in public administrations are able to carry out regular cloud audits.

5.4 Research Field III: Cloud Utilization

This part of the dissertation examines the status quo regarding the use of public cloud services and the associated aspects of information security in e-government. The goal is to generate and process well-founded results in this application domain in order to close the existing research gap. Paper P6 presents the results of the online survey of local authorities in Germany.

[P6]: Utilizing cloud services in local governments as digital transformation booster by mastering information security duties

Extensive literature research has shown that there are currently very few scientific publications available that have dealt with the usage behavior of cloud computing in public administrations in Europe. In Germany, KPMG has so far regularly examined the use of cloud computing in the industry application domain [36]. However, public administrations have not been taken into account. Overall, there is no study data available on how public cloud services are used in public administrations in Germany.

In order to tackle this research gap, a comprehensive empirical study was conducted in 2023 to answer both research questions **RQ4** and **RQ5**. As it became clear from the outset that such data collection would be time-consuming, both research questions were addressed together on the basis of one web-based questionnaire. CISOs and ICT managers from local authorities were involved in a multi-stage process in order to concretize relevant questions and hypotheses. The questionnaire was designed according to a scientific approach and adapted to the target group. As it was not possible to directly advertise this study through central state authorities for organizational reasons, the public administrations at local authority level had to be contacted by e-mail. For this purpose, a comprehensive address list was generated and prepared with the support of a self-programmed web crawler. ID numbers for each local authority were integrated into this list so that an automated e-mail reminder could be sent to local authorities that had not yet taken part. Overall, a good participation rate was achieved under these conditions in order to be able to derive valid results. The online survey was conducted in the period from 01.08.2023 to 30.11.2023. After quality assurance, the responses from a total of 507 local authorities were taken into account for this study (see Table 4).

Federal state	Cities > 200 inhabitants	Participating municipalities	Participating municip. (rel.)	Adoption of PCS	Adoption of PCS (rel.)
Baden-Württemberg	1.095	75	6,8 %	61	81,3 %
Bayern	2.056	111	5,4 %	88	79,3 %
Berlin	1	1	100,0 %	0	0,0 %
Brandenburg	413	21	5,1 %	16	76,2 %
Bremen	2	0	0 %	-	- %
Hamburg	1	1	100,0 %	1	100,0 %
Hessen	422	54	12,8 %	38	70,4 %
Mecklenburg-Vorpommern	692	10	1,4 %	7	70,0 %
Niedersachsen	941	44	4,7 %	36	81,8 %
Nordrhein-Westfalen	396	69	17,4 %	52	75,4 %
Rheinland-Pfalz	1.914	31	1,6 %	20	64,5 %
Saarland	52	8	15,4 %	7	87,5 %
Sachsen	419	38	9,1 %	29	76,3 %
Sachsen-Anhalt	218	13	6,0 %	10	76,9 %
Schleswig-Holstein	967	9	0,9 %	7	77,8 %
Thüringen	546	22	4,0 %	18	81,8 %
	10.135	507	5,0 %	390	77,0 %

Table 4: Participating local governments and adoption intensity of public cloud services.

The participating municipalities were divided into three groups depending on their number of employees: small (25.3%), medium (50.4%) and large (24.4%). In total, 77% of the participants surveyed already use at least one public cloud service in their organization. Public cloud services are most frequently used for the following applications: file sharing service (32%), council information systems (22%) and G2C portals for e-government (13%). PII is processed in all of these public clouds, making the significance for information security management particularly relevant. Almost 50% of the local authorities surveyed do not currently have up-to-date cloud documentations. This means that these organizations are highly unlikely to be in a position to establish adequate cloud security management processes (see Figure 12).

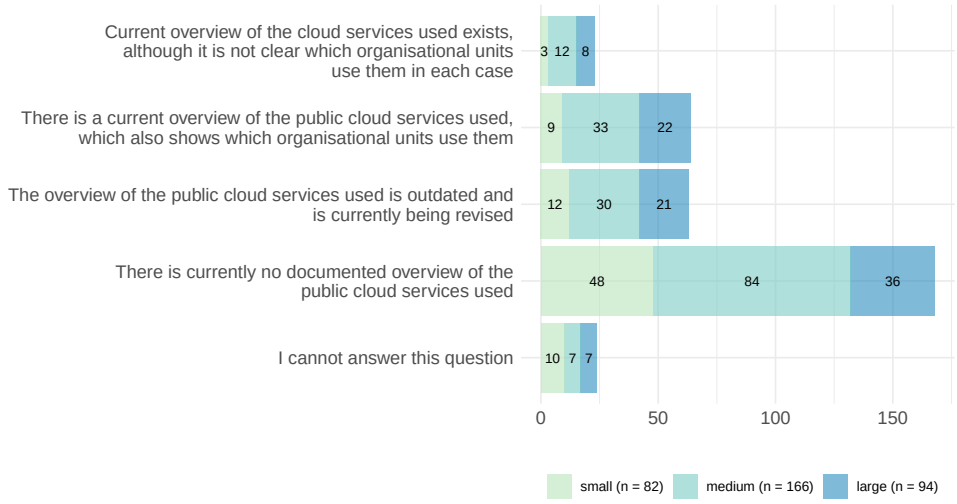


Figure 12: Documentation of public cloud services in local governments.

Furthermore, the results show that there are hardly any cloud security policies that specify the requirements of the BSI IT-Grundschutz (see Figure 13). For example, only 23% of the study participants which use public cloud services currently have specific regulations covering regular reviews of access permissions in public cloud services. The fewest respondents have instructions for the regular review of subcontractors, service level agreements and compliance requirements

German authorities have a lot to do when it comes to implementing cloud security requirements. There is currently a lack of concrete IT security policies for public cloud services. The documentation of the cloud services deployed is also missing or incomplete in many local authorities. There is little or no organizational and technical preparation for the future implementation of Microsoft 365 as a public cloud service. It is currently hoped that on-premise software will continue to be offered and that a migration to public cloud services can be avoided. The hypotheses tested showed that there is a very strong correlation between the existence of a cloud strategy and the associated IT security policies.

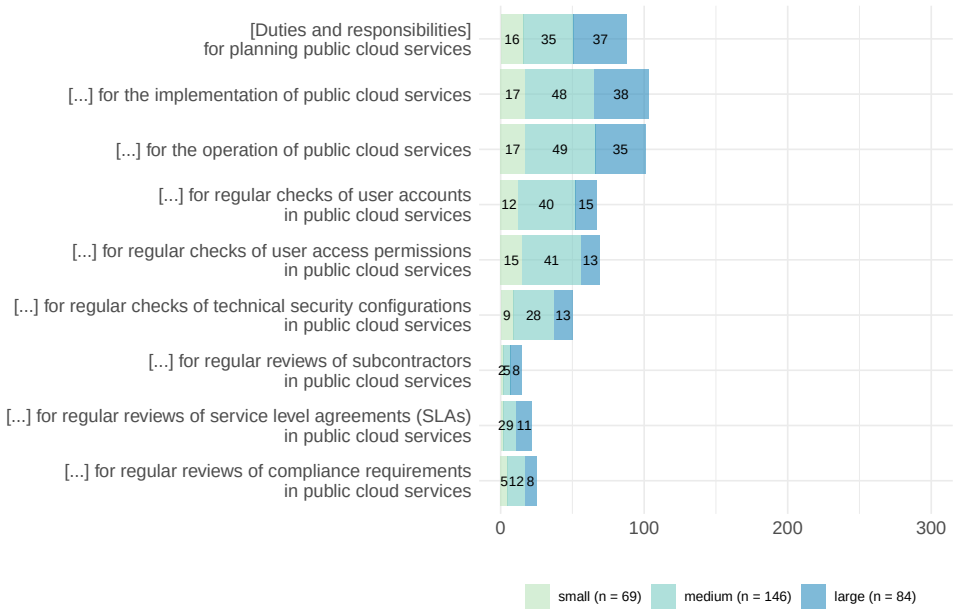


Figure 13: Number of regulations for managing the information security of public cloud services in municipal administrations (multiple answers possible).

Contribution: The results of this representative study show that public administrations in Germany need individual cloud strategies as quickly as possible and must implement the requirements of the BSI IT-Grundschutz Compendium (ORP.2.2 Cloud Usage [11]) or comparable security frameworks. On the one hand, in order to establish the security management of public cloud services, and on the other hand, in order to be able to use the cloud potential in the digital transformation in eGovernment in a meaningful way. The results suggest that the potential of public cloud services has not been recognized and that inadequately secured clouds are massively vulnerable to cyberattacks.

5.5 Complementary Publications

In addition, the content of this dissertation was influenced by the involvement in further research activities. Table 5 provides an overview of these publications, consisting of a conference paper (C) and a journal article (J).

No.	Publication	Type	State
C1	NETTER, M., WEBER, M., DIENER, M., PERNUL, G. (2014). Visualizing Social Roles-Design and Evaluation of a Bird's-Eye View of Social Network Privacy Settings. In *Proc. of the 22nd European Conf. on Information Systems (ECIS)*, Tel Aviv, Israel, pp. 776-785.	C	published
C2	DIENER, M., KRAUS, A., FISCHER, L. (2016). Einsatz von Cloud Computing in deutschen Unternehmen: Status quo und Bedeutung der Informationssicherheit. In *Journal Banking and Information Technology (BIT)*, 17(1), pp. 44-53.	J	published

Table 5: Overview of complementary publications.

Before the focus of this dissertation was placed on the area of cloud computing security, collaboration took place on a laboratory study for a visualization tool for access rights in a social network (publication C1). With the help of several test subjects, it was shown that a visual representation of complex relations can significantly help end users to improve their own security configurations in a system. The findings from this study were partly incorporated into the development of the dashboard visualization (Paper P5).

In addition, an online survey was conducted to analyze aspects of information security when it comes to cloud computing in industrial environments (publication C2). When carrying out the study, it became clear that a high response rate is not a matter of course. High-quality study results can only be achieved by addressing the target group correctly. This experience helped considerably in the preparation and implementation of the survey in Paper P6. In terms of content, this study revealed that although the respondents were able to correctly assess the necessary protection requirements for given data categories, most respondents found it difficult to create an overview of the data storage locations where these data categories could be found. These findings led to the development of the Cloud Data Inspector in Paper P1.

6 Conclusions and Future Work

Cloud computing will massively drive the digital transformation of public administrations in the next few years. The operation of in-house data centers in municipal institutions will have to be rethought, as the economic and technical advantages of using external cloud resources will prevail. The costs for IT operations at local data centers and for personnel will increase significantly, meaning that the cost efficiency of public cloud services will play a role in any procurement. The fact that there will be a shortage of IT specialists in public administration in a few years is problematic. Management will therefore be forced to turn to outsourcing and cloud solutions in order to provide business processes with high-performance IT resources. Many resources are currently being invested in the development of the DVC. It has the potential to provide trustworthy cloud services for government institutions. However, it will take a long time before these cloud services can be adopted from the DVC marketplace. Since Covid 19 at the latest, municipal administrations have started to adopt public cloud services that are operated by private companies. At that time, public cloud services were not available to administrations at the local level, e.g. video conferencing, file sharing, collaboration portals for processing sensitive data between citizens and companies. As a result, clouds were introduced autonomously in every government agency. Furthermore, the pressure on IT management in public administrations has been increasing for a few years now, as more and more software manufacturers are offering their products as cloud services. Public administrations currently have to deal intensively with the question of how the security and data protection of apps from the Microsoft M365 public cloud can be implemented organizationally, technically and legally. It is urgent that local authorities address the information security of public cloud services. Pragmatic and simple security concepts are needed to ensure the successful integration and operation of public cloud services. Public administration is lagging far behind the private sector in these technological developments, which dramatically increases the risk of adopted public cloud services having potential security vulnerabilities. This scientific work has dealt intensively with these problems in recent years. For this purpose, three research fields were defined in this dissertation, which address the following sub-problems.

The focus in Research Field I was on *cloud security management*. Design science research was used to construct innovative software tools that can make a valuable contribution to solving the aforementioned problems. The tools developed addressed several facets. The Cloud Data Inspector supports decision-makers in selecting the appropriate public cloud service based on automated data classification using a machine learning model. Dynamic decisions are made taking into account predefined cloud security policies. In addition, methodical approaches with tool support will play a decisive role in the future in order to be able to regularly check the compliance of the public cloud services used. Therefore, a tool was developed that visually displays the status quo of the information security maturity level in a dashboard. This gives CISOs in public administrations the technical ability to systematically identify vulnerabilities in documented public cloud

services. On this basis, technical and organizational security measures can be initiated at an early stage.

Research Field II investigated the impact of *cloud audits* in the public sector. Security audits are the basis for regularly reviewing security requirements for public cloud services. In a first step, the available cloud certifications were examined with a comprehensive literature research. It was found that the EUCS certificate offers a promising approach for the public sector. However, this is not yet available for productive use. Furthermore, conducting in-house cloud audits is unavoidable. In this dissertation, the web-based tool Cloud Inspector has been developed, which integrates the responsible employees of public cloud services into the holistic process of information security management. The methodical approach takes into account that clouds can be used decentrally in organizational units.

Cloud utilization was examined in Research Field III. For this purpose, the status quo regarding the utilization of public cloud services in municipal administrations in Germany was investigated as part of a comprehensive online survey. The results show that the use of public cloud services is highly widespread in this domain. However, there are significant shortcomings with regard to the existence of cloud strategies and cloud security guidelines in the government institutions.

Overall, this dissertation has produced new scientific findings using design-oriented and empirical research methods. By incorporating this new knowledge, the practical concepts of information security in public administrations can be enhanced in order to protect public cloud services from cyberattacks. At the same time, the results can be taken up and further developed in research. However, possible future research areas were identified during the course of this dissertation.

Firstly, there needs to be a systematic investigation into the cloud hyperscalers that exist in Europe today meeting the security and data protection requirements. This involves investigating how these can be integrated into the DVC, Gaia-X or IPCEI-CIS. In this context, it is also necessary to analyze how authorities can identify public cloud services in these ecosystems that meet the defined technical, organizational and legal conditions. The use of dynamic cloud certifications is particularly relevant in this conjunction.

Secondly, there is an open research gap regarding the integration of public cloud services into SOC infrastructures. In particular, SaaS and PaaS solutions without API access have so far been established in municipal administrations. This raises the question of how such cloud services can be automatically and regularly monitored by implementing real-time risk management frameworks with proactively controlled cloud risk treatment processes. It is also necessary to investigate how structures and concepts (e.g. SASE) can be improved to efficiently operate SOC infrastructures for public administrations in Germany.

Thirdly, with regard to BCM, cloud emergency strategies and playbooks are necessary in local SOC departments so that business processes that are dependent on public cloud services are still minimally functional in the event of cyberattacks or technical faults.

Part II

Research Papers

1 Tackling the cloud adoption dilemma - A user centric concept to control cloud migration processes by using machine learning technologies

Publication details:

Status:	Published
Conference:	11th International Conference on Availability, Reliability and Security, ARES 2016, Salzburg, Austria, August 31 - September 2, 2016
Date of acceptance:	May 30, 2016
Full citation:	DIENER, M., BLESSING, L., RAPPEL, N. (2016). Tackling the cloud adoption dilemma - A user centric concept to control cloud migration processes by using machine learning technologies. In *Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES)*, Salzburg, Austria, pp. 776-785.
Authors' contributions:	Michael Diener 70% Leopold Blessing 20% Nina Rappel 10%

Conference description: The International Conference on Availability, Reliability and Security will bring together researchers and practitioners in the area of dependability. ARES will highlight the various aspects of security – with special focus on the crucial linkage between availability, reliability and security. ARES aims at a full and detailed discussion of the research issues of security as an integrative concept that covers amongst others availability, safety, confidentiality, integrity, maintainability and security in the different fields of applications.

Tackling the cloud adoption dilemma - A user centric concept to control cloud migration processes by using machine learning technologies

Michael Diener, Leopold Blessing
Department of Information Systems
University of Regensburg, Germany
michael.diener@wiwi.uni-regensburg.de
leopold.blessing@t-online.de

Nina Rappel
Chair of general business studies
Brandenburg University of Technology
Cottbus-Senftenberg, Germany
nina.rappel@b-tu.de

***Abstract*—Research studies have shown that especially enterprises in European countries are afraid of losing outsourced data or unauthorized access. Despite various existing cloud security mechanisms companies are currently hesitating to adopt cloud resources. This phenomenon is also known as cloud adoption dilemma. We think that data classification is a promising technique that should be considered in the context of cloud security, supporting cloud migration processes. By using classification techniques enterprises are able to control which documents are suited for Cloud Computing and which cloud service providers are sufficient for protecting sensitive documents. In this work we present an efficient concept that involves enterprises' employees and authorities, making it possible to apply powerful security policies in a simple way. We make use of a well-established machine learning algorithm in our developed tool, identifying security levels for different types of documents. Thus, cloud migration processes can become more transparent and enterprises obtain the ability to discuss more openly about adopting innovative cloud services.**

***Keywords*-cloud computing, cloud security, cloud adoption, cloud migration, machine learning, supervised learning, naive bayes classifier, data classification, user centric tool**

I. Introduction

Cloud Computing nowadays has become one of the most important paradigms and is tremendously affecting the Information and Communication Technology (ICT) more than any other IT topic [1]. Since Google's CEO Eric Schmidt had coined 'Cloud Computing'[1] in 2006 in the context of distributed services over the internet, technologies like virtual machines, huge online storages and sophisticated services for mobile apps have been created. As global ICT players like Amazon, Apple, IBM, etc. jumped on the bandwagon by starting to develop innovative products and services that are connected with the web, the trend of Cloud Computing is still going on.

By 2009, Armbrust et al. already had stated that cloud technologies may possess the potential to change the way software and hardware is constructed and purchased [2]. From the economic point of view, the authors mentioned that cloud-based services may constitute interesting opportunities for make-or-buy decisions. Another opinion with respect to Cloud Computing is represented by Buyya et al., who believe that computing in general will be the 5th utility behind water, electricity, gas and telephony [3]. By adopting cloud-based services, consumers are able to use various kinds of digital products from data centers which are geographically distributed all over the world. Consumers only need to pay for the services they have used, thus it becomes needless to buy expensive hardware or software to perform temporary computing tasks.

Meanwhile it has become obvious that Cloud Computing is a major driver that can significantly strengthen enterprises' competitiveness [4], [5]. By adopting the cloud, companies can conceptualize innovative IT products by themselves. Especially for small businesses it is important to be able to enhance their innovation and collaboration activities in order to be competitive [6]. Due to the fact that these companies do often have only limited financial and infrastructural resources, they are dependent on technologies that are able to meet their requirements. Cloud Computing is a technology that allows companies to adopt specific resources from a wide range of cloud-based services like high-performance machines (Infrastructure-as-Service), programming environments (Platform-as-a-Service) or ready-to-use applications (Software-as-a-Service) [1].

However, in order to be able to benefit from the advantages of Cloud Computing it is commonly necessary to migrate data into external data centers, hosted by Cloud Service Providers (CSPs) [7], [8]. As soon as CSPs have received data, the processed data normally remain in the systems of a Cloud Service Provider (CSP). Thus, security issues are often discussed in scientific publications, as the protection of data within external systems is an essential aspect of Cloud Computing [2], [9], [10].

Because of the fact that data are no longer hosted within local systems, some authorities of enterprises fear incidents of unauthorized access to their data. In literature this situation is also known as the dilemma of cloud adoption [11], [12] because on the one hand enterprises have an enormous interest to use cloud services, on the other hand they are afraid of this technology. This effect can mostly be observed in some European countries (e.g. Germany), where companies often hesitate to adopt cloud services [13].

We believe that these companies will be more open to cloud adoption if they possess a deep understanding of the sensitivity level of their data, knowing that critical information will not unintentionally be hosted within cloud

[1] http://www.google.com/press/podium/ses2006.html

services. In order to validate our hypothesis we conducted an expert interview with over thirty participants from different enterprises [14]. As a result, we could prove that there is a close relation in between data types, i.e. human resources records and their associated sensitivity level (highly confidential vs. less critical). Most participants classified the presented data types as we had expected. Public documents like brochures or press articles have been seen less sensitive in contrast to CAD-files, customer records, and supplier contracts. To our surprise we recognized that in most companies the identification of storage locations of highly confidential data averagely lasts up to more than one day. Moreover, most companies of the participants do not have a security policy that controls which of companies' data are allowed for data processing in cloud environments. Thus it becomes clear, that enterprises are often aware of the sensitivity level of their processed data types, but they are not able to efficiently identify these data in their hay stack. We think that this might be a possible reason why companies have fears to use cloud services. Against the background that data volumes will be increasingly growing over the next years, powerful and easy to use solutions are required. It is important that staff is supported in an efficient way, so that companies are able to reduce their fears against cloud-based data processing.

In this work, we are presenting a concept that is able to improve users understanding of the sensitivity level of local data by developing a user centric tool that suggests whether data are uncritical for data processing in the cloud or not. We implemented a supervised machine learning algorithm in our tool that can be easily trained by users themselves, assigning a certain sensitivity level. As far as further data should be transferred into the cloud, the trained model can be reused in order to support the user in an efficient way to determine whether the analyzed data are suited for cloud migration. In this way, we want to involve the user in the data analysis process and as a consequence reduce the users' fears against cloud adoption.

The remainder of this paper follows the design science research paradigm considering the guidelines for applying design science research by Hevner et al. [15]. Within our research we make use of the process model of Peffers et al. [16] which supports the guidelines provided by Hevner et al. In Section II, we describe the context of the problem and related work, emphasizing the research gap we have identified. Based on this, we briefly illustrate in Section III how a machine learning classifier can be used for document classification. In Section IV, we will present our concept that supports within the cloud migration process, enforcing that only those documents are migrated into specific cloud environments that are uncritical. In order to illustrate how our concept can be applied in practice, we have developed a small prototype called Cloud Data Inspector, including a naive Bayes classifier and a security policy manager, guiding users through the cloud migration process. After that we evaluate the efficiency of our prototype by conducting a laboratory experiment with a few employees from regional companies, investigating the impact of the underlying approach to a users behavior with respect to cloud adoption in their enterprise. In Section VI, we point out the contribution of our work and discuss challenges of the problem context which we want to tackle in future research work. Finally, Section VII sums up our research work.

II. Related Work

Currently, the amount of cloud services is tremendously increasing, so that it is becoming very complex to identify a suitable one, because every CSP has its own specific features and characteristics. The idea of using only one trustworthy CSP does not work in reality because of the diverging requirements of customers, suppliers and business partners (e.g. identity management issues). Thus, the adoption of cloud services is closely linked to a variety of factors which decision makers need to evaluate before they select a specific CSP who communicates with their business processes. These factors cover especially the pricing model, features, performance, scalability and most importantly, security [17].

Our research is focused on data security as it is the most challenging factor that needs to be tackled when it comes to cloud computing in enterprises from our point of view [18]. In the following, we will give a short overview of technological approaches to securing data in cloud infrastructures. In addition we also have a look on cloud adoption frameworks, supporting decision makers in finding a suitable CSP. In times of continuously growing data volumes it becomes difficult to keep track of the sensitivity of specific data. Algorithms which are used for machine learning are promising to perform automatic text classification. In the last part of this section we point out the research gap and formulate objectives in this work.

A. Security for Cloud Computing

With reference to security in cloud infrastructures, by now an uncountable number of publications by international researchers exists, proposing novel approaches and techniques to enhance cloud security. What is needed are approaches so that data owners or decision makers obtain the ability to assess security guarantees of CSPs [10]. However, in reality developing adequate mechanisms that demonstrate an achieved high level of cloud security of a certain CSP is a challenge [19]. Modi et al. investigated different layers of cloud environments, evaluating possible vulnerabilities and attacks, and identified adequate solutions to enforce cloud security [20].

A promising solution is encryption that is usually implemented in existing cloud services, enforcing data integrity and securing data against unauthorized access. The EU funded research project PRISMACLOUD focuses on cryptographic concepts and methods in order to enhance security and privacy issues in context of cloud-based services [21]. In addition, some European solutions like *boxcryptor.com* or *cloudfogger.com* are still available.

These services encrypt data before they are transferred into cloud storages. As a consequence, users have to trust that the software of CSPs, which is required for end-to-end encryption, does not contain any backdoor [22]. Therefore one essential question still remains regarding companies using Cloud Computing [23]: who is able to access the encryption key? Therefore, another type of data encryption becomes more and more interesting. Those are homomorphic techniques that allow processing information on encrypted data [24], [25]. Thus, it is much more complicated for a CSP to access external data of his customers. However, SQL queries that contain wildcards cannot often be executed efficiently on encrypted data. Alternative techniques like fuzzy keyword search [26] are necessary or a holistic approach like CryptDB is required [27], leading to the effect that the desired data protection has negative impacts on the original idea of Cloud Computing [10]. In order to make sure that the privacy of highly sensitive data, for example customer information and payment data, is guaranteed, it has been proved that it is possible to combine encryption with fragmentation techniques [28]. Another technology that is indispensable when it comes to Cloud Computing is identity management which ensures that only authorized users have access to specific parts within a cloud environment [29], [30], [31], [32].

Moreover, secure cloud environments cannot only be achieved by implementing encryption. Due to the fact that numerous customers of a CSP are using the same underlying infrastructure, it is essential that CSPs are able to prevent malicious activities, i.e. DDoS-attacks against the connected systems. Also CSPs are responsible for identifying malicious developments in their cloud infrastructure. Therefore, intrusion detection systems (IDS) and security information and event management (SIEM) are becoming important research fields [33], [34], [35].

Despite available security measures, customers have to trust that the CSP is able to protect their entrusted data in the best possible way. In particular, regarding processing sensitive enterprise data, the selection of an adequate and trustworthy CSP can become very complex, because various characteristics of different providers have to be taken into account [36], [17], [37], [38], [39]. In general, most of the proposed cloud adoption frameworks provide a self-assessment for evaluating specific criteria of CSPs. However, in our opinion the general problem of these frameworks is that the current state of the suitability of a certain CSP has to be continuously evaluated in order to be able to respond appropriately and quickly. Additionally, the sensitivity level of data or documents is often not considered by these self-assessment approaches. Therefore we focus on machine learning, as it is able to automatically classify enormous amounts of data very efficiently.

Taking everything of the above mentioned in account, outsourced data are no longer within the control area of their data owners as soon as they have been migrated to external cloud environments. In conclusion, it is essential that authorities in enterprises keep track of their data before they are migrated into cloud services, so that a valuable contribution to the cloud adoption dilemma can be achieved. With respect to our conducted study [14] we are convinced that an enhanced understanding of data sensitivity is a promising approach to make the cloud migration process more transparent [40].

B. Machine Learning

Machine learning affects various research fields, i.e. speech and text recognition, medical diagnosis or search engine development, whereas the underlying algorithms are used for detecting similarities, outliers or clusters. However, in order to find accurate results in raw data it is absolutely necessary to identify appropriate machine learning algorithms which can deal with a specific problem.

In general three machine learning methods are widely known today: supervised, unsupervised and reinforcement techniques [41]. Reinforcement learning focuses on the method of teaching an autonomous component (i.e. agent) which acts within a specific domain to choose best-fitting actions in order to achieve pre-defined goals. Neural networks built an important basis for performing such operations. Unsupervised learning methods like k-Means provide data analyses without pre-trained models. The automatic generation of clusters is a typical approach towards unsupervised learning. In general, the clustering algorithm requires raw data to be analyzed and the amount of clusters that should be generated for the analysis.

In contrast, supervised learning is a typical field for classification activities, i.e. assigning classes or labels to data which can be characterized by specific properties [42]. In a first step a computational model will be manually trained by using parts of data and pre-defined classes. During this phase the algorithm learns to assess the characteristics of the data that are delivered to its input interface. In a second step, the algorithm takes the generated training model and further test data. After completion, the result contains a list of relationships between the investigated data items and one or more related classes. Naive Bayes is a famous algorithm that is used for supervised learning tasks and automated text classification [43].

C. Research gap

Although numerous security techniques that can protect data in cloud environments are existing, companies' fears will still remain because the question has not been answered which of their data are uncritical for cloud computing [14]. The aforementioned security measures such as encryption can provide mechanisms to safeguard data in the cloud. Although frameworks and tools are supporting decision makers to identify suitable and trustworthy CSPs, they cannot help in the case of enterprise data getting lost or stolen by unauthorized data access [13]. Therefore it is no surprise that some decision makers are of the opinion that their files are better secured if they are located in their own systems [40].

Correspondingly, companies might be more open for cloud computing when they have the ability to understand which data are harmless for data processing in

external systems. The proposed scientific contributions in subsection A are answering this crucial question to a limited extent only. To the best of our knowledge we cannot identify attempts in the research community to provide end-users with mechanisms that help them to understand their data for cloud migration. In this work, we are using machine learning in order to present outputs for decision makers, affecting their attitude to cloud migration in a positive manner. We provide a generic concept that allows authorities in enterprises to decide which data are uncritical for data processing in the cloud. Based on this we demonstrate the functionality of our solution by creating a prototype that classifies enterprise documents. The objectives of our idea are as follows:

- We want to make the cloud migration process more transparent by analyzing data that are intended for cloud computing.
- We want to design a concept in a way that directly involves end-users in the analysis process, thus their trust in cloud computing can be increased.

III. Naive Bayes Classifier

As mentioned in the previous section a famous algorithm that implements the supervised learning approach is the naive Bayes classifier, implementing the idea of the Bayes' theorem which implies that each document belongs to a specific class with a certain probability $P(c_j|d)$, whereby c_j is representing the class and d one document.

$$P(c_j|d) = \frac{P(c_j) \cdot P(d|c_j)}{P(d)} \tag{1}$$

The algorithm calculates each possible probability of which a document might belong to a certain class and assigns the considered document to the class with the highest probability value:

$$\gamma_{NB}(d) = arg_{c_j \in C} max P(c_j|d) \tag{2}$$

In general, a naive Bayes classifier assumes that all words in a text are independent from each other while in reality this assumption is 'naive' in most cases. In the process of considering all words of a text, the position of specific words is completely disregarded by a naive Bayes classifier. In order to be able to calculate probabilities it is necessary to tokenize a text or document into single words. This can be conducted on the basis of a so called bag-of-words model which counts the frequency of a unique word within a specific document. The columns contain the different documents, whereas the rows represent unique tokens that are extracted from the documents. The idea of this model can be depicted by a two-dimensional matrix, displaying the frequency of words within documents (cf. Table I).

For example, document d_3 is characterized by two unique words, whereas the token 'secret' is included five times and the token 'contract' four times. Moreover, this model can be enhanced by adding a single row containing a unique class that is related to a specific document. In this case, the class 'sensitive' is associated to document d_3. Based on such a representation, it is possible to train an algorithm in order to determine whether the evaluated document belongs to a specific class or not. Therefore it is necessary to enhance the aforementioned mathematic formula so that the frequency of words within a class can be considered, also known as a multinomial naive Bayes classifier:

	d_1	d_2	d_3	d_4	d_5
secret	3		5		
contract	2		4		5
press		3		2	
release		3			
address	1	2		4	1
information	6	3		1	6
class c	sensitive	¬ sensitive	sensitive	¬ sensitive	sensitive

Table I
BAG-OF-WORDS MODEL USED FOR TRAINING A CLASSIFIER

$$\gamma(d) = arg_{c_j \in C} max \left(\frac{g_j}{|D|} \cdot \prod_{t_k \in d} \left(\frac{tf_{c_j}(t_k)+1}{\sum_{t_i \in V} (tf_{c_j}(t_i))+|V|} \right)^{tf_d(t_k)} \right) \tag{3}$$

The formula consists of the following parameter: D is the amount of the used training documents and C the number of different classes, whereby g_j is the number of training documents that refer to class c_j. V represents the vocabulary of the used terms and contains the number of unique words over all classes. The terms $tf_{c_j}(t_k)$ and $tf_d(t_k)$ refer to the frequency of a specific word in a class or a document. Because of the fact that the numerator of the formula can be zero in case the word frequency is null, it is necessary to integrate Laplace smoothing.

Thus, it becomes clear that a multinomial naive Bayes classifier is useful in order to determine possible probabilities of words in different documents, determining a certain class a document belongs to [44]. Therefore in a first step, a training model as it is shown in Table 1 has to be generated. On the basis of this training model further unlabled documents can be classified, as Figure 1 shows.

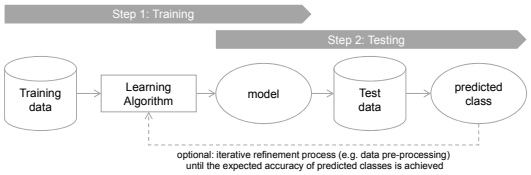


Figure 1. Supervised learning process based on [44]

In general, a naive Bayes classifier can be used for various problems. A well-known example for the application of such a classifier is a typical spam filtering mechanism in email programs. In a first step a user has to tag several emails that from his point of view contain spam content. After training, the algorithm can be applied to incoming mails and as a result detected spam mails get moved or deleted. We will use this mechanism to support users

so that they are able to associate documents to different classes, for example sensitive or non-sensitive documents.

IV. Supervised learning for cloud migration control

In this section, we present our user centric concept supporting users to understand their data more deeply from the security perspective. Based on the supervised learning process and a visual feedback by our tool we identify similarities between training and test documents, providing the user with enhanced information about the required sensitivity level. This section is divided into two parts: in the beginning we will give a conceptual overview of the idea of our concept, controlling the cloud migration process with the help of supervised learning. In order to demonstrate how the proposed concept can be applied in practice we have developed a user centric tool. In part B of this section we demonstrate the functionality, inspecting typical documents that are common in daily business.

A. Conceptual design

In general, documents commonly contain more or less sensitive data. However, whether an information is sensitive or not depends on a set of security policies that have to be predefined and maintained over the time. In practice it is common to tag documents with a security level (e.g. top secret, secret, internal use, public) in order to activate related security mechanisms on organizational and technical layers. Based on this security labeling it is possible to control the information flow between different organizations, departments and systems. Nevertheless, it might become very difficult to instantly determine an adequate security level for a specific document, if such a classification tag is not assigned already. From enterprise authorities' point of view, the migration process into Cloud Computing is insecure and intransparent, as it is not clear to them which data are moved to external servers, and which are not. As a consequence, this situation often influences decision makers in a negative way, thus the dilemma to adopt cloud services is happening.

Due to this dilemma and the aforementioned problem context, our concept follows the idea to support users and authorities of enterprises in a user centric way, so that a direct connection between a document and a possible CSP is established, regarding security levels and transparency in the cloud migration process. The idea is based on the principle that employees do not need to know details about the content of documents or files. The only thing users do have to recognize is the class or the type of a document (e.g. invoice, contract, press release, CAD, or human resources data) that describes the documents characteristics best. In this context we suggest that only a few classes are defined so that employees will keep the overview about the relations between documents and classes, for example a *supplier contract* relates to the class *contract*. To achieve the intended efficiency and transparency within a cloud migration process, our concept provides a mechanism that allows employees to easily train a machine learning model by simply adding documents to predefined classes. This makes it possible that employees are directly involved in security issues within cloud migration processes, because they obtain technical knowledge to describe which documents relate to a specific class. Figure 2 shows which activities a user has to do in order to train the machine learning model.

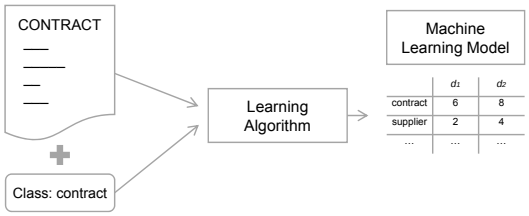


Figure 2. Training the Machine Learning Model

In contrast, authorities who need to decide whether data are suited for cloud data processing or not, only have to assign specific security levels to document classes. We assume that they do have a broad overview about security and compliance issues of an enterprise, being able to model security policies that can describe the preferred cloud migration process. Therefore it is necessary to assign these document classes to predefined security levels. A security level (i.e. public) specifies, which security measures are required to achieve the preferred security in cloud migration processes. Provided that certain CSPs are trustworthy and compliant with the preferred security measures, it is possible to assign them to those security levels. Finally, our approach is able to link various enterprise documents with secure and trustworthy CSPs, influencing the cloud migration process in a secure and transparent manner. Figure 3 shows an abstract entity relationship diagram that formalizes the proposed dependencies between the described elements.

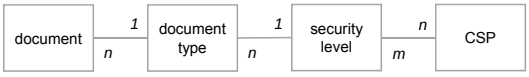


Figure 3. Dependencies between documents and CSPs

By using our concept to control cloud migration it is possible to shape a seamless and secure chain between single documents and trustworthy CSPs, thus it can be determined which cloud environment is suited for processing specific documents. In this respect, responsible security employees can formalize security policies, which prevents migration of highly sensitive document types to insecure CSPs. Moreover, our proposed concept is able to guide employees in their daily business to use Cloud Computing in a secure way, contributing a small but valuable step of security that can help to solve the cloud adoption dilemma. In the following subsection we will explain how our proposed approach can be digitized.

B. Cloud Data Inspector

In order to demonstrate that our proposed concept is working, we have developed a small prototype which we have named “Cloud Data Inspector”. The tool is divided into three main functions: Document Inspection, Model Training and Policy Management. We have programmed our tool in Java, offering an easy to use graphical user interface. The tool can be used by employees and authorities that are involved in the cloud migration process. The Cloud Data Inspector builds the boundary between a user who wants to migrate data and predefined CSPs. Thus, our tool can support enterprises in a secure and transparent way whenever data are leaving the company to external CSPs.

1) Policy Manager: In a first step, authorities are requested to configure security policies within the Cloud Data Inspector. Therefore it is necessary to add document types and security levels to our tool. In a second step the relation between document types and security levels needs to be modeled. On the basis of the proposed ERM in figure 3, a possible configuration can look like as it is shown in Table II.

document type	**security level**
Invoice	Extranet
Contract	Secret
Press release	Public
CAD	Secret
HR data	Top Secret
Price calculation	Top Secret
Organizational instruction	Extranet

Table II
SECURITY POLICY: RELATION BETWEEN DOCUMENT TYPES AND SECURITY LEVELS

Furthermore, the relation between a security level and one or more suitable CSPs needs to be configured. A security level can be assigned to more than one CSP as it is possible (e.g. due to historical conditions and ongoing projects) that different service providers are already in use that are complying the expected security measures linked with the security levels. In Table III we outline how such a definition can look like.

security level	**CSP**
Public	ownCloud, MagentaCLOUD, Dropbox
Extranet	ownCloud, MagentaCLOUD
Secret	ownCloud
Top Secret	–

Table III
SECURITY POLICY: RELATION BETWEEN SECURITY LEVELS AND CSPS

As it can be seen in this table the security policy prevents that data types that are classified as top secret (e.g. HR data, price calculations) are leaving the company. If there is an attempt to transfer those files towards a cloud environment, the Cloud Data Inspector will show a warning that this action is aborted due to security policies. Files like contracts or CAD data which are used for project management with external partners are only allowed for migration to a secure and trustworthy CSP like the Deutsche Telekom Cloud. However, if employees do not use the Cloud Data Inspector it is also possible to transfer sensitive files to untrustworthy CSPs. At this point the implementation of Data Loss Prevention (DLP) or SIEM systems is required, preventing that sensitive data are leaving the company. Therefore a data export interface is required in our tool, so that it is possible to access security policies and training models that describe the configured security settings in a machine readable format.

2) Model Training: The application of our model training process in the Cloud Data Inspector is rather easy to use. Common files and documents can be added to our tool by drag and drop. After a file was recognized, the information extraction process starts. For this process we use *Apache Tika*[2] which is able to extract content out of various files, for example Microsoft Office or PDF documents. Depending on the size of a file the extraction process takes only a few seconds to provide the Cloud Data Inspector with the extracted raw data.

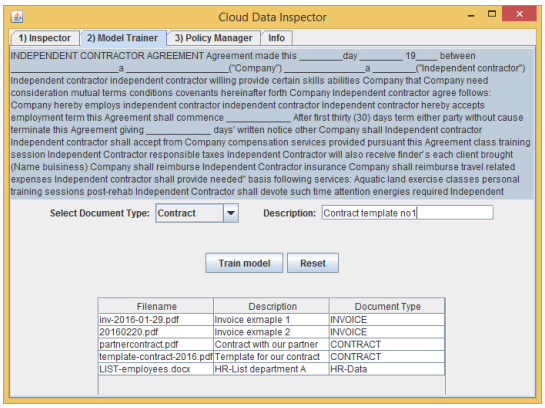


Figure 4. Training the learning model by adding a contract

As soon as the plain text is visible, the tool requests the user to associate a suitable document type to the inspected document. At this point, two important input parameters are given, which are required to adjust the learning model with this document and this document type (cf. figure 2). The training process starts when the button ‘Train Model’ is pressed, conducting our self-programmed naive Bayes classifier. The results of the training process will be saved to a CSV file so that the generated training model can be reused by the inspector component. By applying our proposed concept in this tool, it becomes obvious that the user is actively involved during the training phase and he is able to decide which document type is fitting for a given document. However, he does not have to know about the structure, keywords, etc. inside this document. At the bottom of this view the user can see which documents have been already examined and which class was assigned to them.

[2]https://tika.apache.org

3) Data Inspector: The main component of the Cloud Data Inspector investigates the content of a document and decides, based on the modeled security policies, whether the file is allowed for cloud migration or not. Therefore, the content of the file is extracted (cf. figure 5, left side) followed by the classification process with the integrated naive Bayes classifier which determines the class with the highest probability. Depending on the security level a document type is referring to, the Cloud Data Inspector displays icons of suitable CSPs that are compliant with the given security level (cf. figure 5, right side).

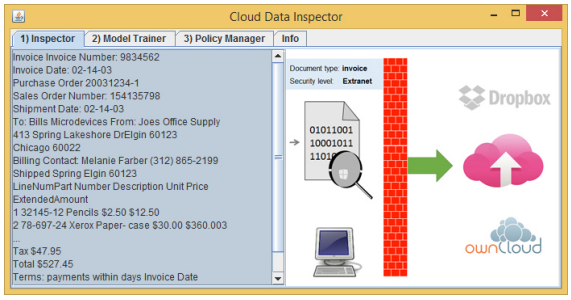


Figure 5. Inspecting a document with the Cloud Data Inspector

In the present case, the user takes an invoice to the Cloud Data Inspector. Based on the configured security policy and the identified document type, our tool informs the user that this document could be migrated to CSPs that are compliant to the security level 'Extranet'. Suitable CSPs are displayed in color, whereas uncertain CSPs are visualized in greyscale. Specifically this means that the user is allowed to migrate the document to the ownCloud or the MagentaCLOUD in the mentioned example. In the case that several CSPs are suitable, the user needs to click on the icon of a cloud instance, starting the cloud migration process of the inspected file. When the user drags and drops a document into the Cloud Data Inspector which must not be moved to external services, like a price calculation, a warning is shown to the user (cf. Figure 6).

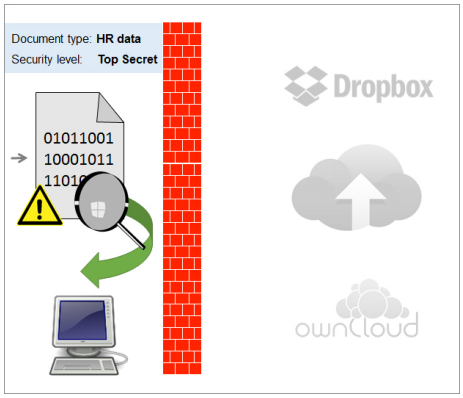


Figure 6. Top secret files are not allowed for cloud migration

In order to make the cloud migration process more transparent, each activity in our tool is logged to a central file. By using the proposed approach in the developed prototype, users are able to interact securely with external cloud resources. In general, the Cloud Data Inspector acts like a middleware between users and external CSPs. Thus the original idea of making the cloud migration process secure and transparent can be realized.

V. Evaluation

The evaluation of our concept and the developed prototype was conducted as a laboratory experiment [45] in order to assess the enhanced transparency of the cloud migration process and the impact on users behavior due to cloud adoption. Our experiment was divided into three steps.

In a first step we have invited 10 users from local companies for our experiment, asking them to identify ten different documents (only Microsoft Word, Excel, Power Point or PDF files) within their IT systems. The users solely knew that the experiment is related to information security. We asked them to select five different documents and characterize them as sensitive or as non-sensitive. In addition, the participants had to write down briefly why they had classified these files as sensitive or non-sensitive in their mind. The users explanation, the related filename and a generic document type (e.g. invoice) was noted on an extra sheet of paper before we met each participant in our department.

In step 2 we explained the idea of our experiment in detail and demonstrated the functionality of the Cloud Data Inspector to the participants. Before we started the experiment, we asked each participant whether they think that the files on their USB flash drive could be migrated to an external CSP. The reaction to this question was no surprise to us: 9 of 10 participants told us that they are unsure about the right selection of a suited CSP that should process their data and they are uncertain whether sensitive files should be migrated from their USB flash drive. One user told us that all files on the USB flash drive had to be kept secret and therefore they would not allow the processing of these data in cloud environments. Regardless, they have classified different files as sensitive or non-sensitive. We encouraged our participants to find solutions to their questions by using our Cloud Data Inspector, training a personalized machine learning model that is able to determine the sensitivity level of inspected documents. Our tool was installed on a single notebook (Intel Core i5 CPU with 2.30 GHz; 8.00 GB RAM; Windows 8.1 Enterprise) which we have used for conducting our experiment. Based on the handwritten results (cf. step 1) the users added the pre-defined document types and the related sensitivity level (sensitive, non-sensitive) to a list in the Policy Manger within the Cloud Data Inspector. In most cases the participants have classified two to three different document types (e.g. telephone list, invoice, offer, instruction manual, etc.). Two participants in our experiment decided to define an additional sensitivity level that is intended to be used for file exchange between business partners. In general, the users are aware of common CSPs

and the related security issues. In all cases, the users linked the option “local processing” to the document type “sensitive files”. With respect to the additional sensitivity level, the two users selected a CSP who operates within the European Union. After that, the users generated their individual training model by copying documents from the USB flash drive to the Cloud Data Inspector, assigning one of the defined document types to each training document (cf. Figures 2 and 4).

In step 3 we investigated the testing component of the Cloud Data Inspector in order to evaluate whether users are comprehensively assisted in the cloud migration process. Therefore, we have simulated if our implemented naive Bayes classifier is reliably able to determine the correct document type by changing some content parts of the original training documents. In general, the participants changed at the minimum five documents. Thus, it is proven that the Cloud Data Inspector uses the characteristics of documents that it has learned in the training phase. Based on the conducted investigation, the Cloud Data Inspector displays the security level and the associated CSP. In all cases, our tool was able to automatically select the correct document class. In order to validate the generated results we have compared them with the participants’ notes on the sheet of paper (cf. step 1). During this process we could observe that 8 of 10 participants feel more secure in cloud migration, because they have seen that our tool suggests security levels they had expected. Two users expressed doubts with respect to our mechanism because it does only focus on the file content and not on significant metadata like author, comments, modify date, etc. However, the mentioned idea of automated document classification is a trustworthy way to emphasize transparency in the information flow between enterprises and possible CSPs.

VI. Contributions and future work

In this paper we showed that our proposed concept of machine learning describes an important step in the right direction to make cloud migration more transparent. The attitude of decision makers can be positively influenced in order to tackle the cloud adoption dilemma. In general, users are aware what kind of documents are more or less sensitive, but this awareness cannot help in times of tremendously increasing data amounts. Continuous data processing leads to the effect that content within files is changing all the time, so that users often cannot be sure which sensitivity level has to be assigned to a document. Hence, a powerful tool like our Cloud Data Inspector can provide employees in an easy way to analyze big numbers of files before they are leaving the companies’ borders.

However, some questions are still remaining to be answered in order to enhance the abilities of our proposed concept. As we have conceptualized our prototype, we had seen that it is possible with Apache Tika to extract further metadata of the inspected documents. By using this valuable information we think it is possible to improve the machine learning algorithm, thus more precise classification results could be achieved. Therefore, in a first step we need to investigate the meaning of specific metadata to understand documents’ sensitivity level by using a comprehensive taxonomy.

Due to the fact that data are continuously changing its content during information processing, we have to research how files that had already been transferred into cloud environments can be monitored. Our tool is currently able to support users solely in the cloud migration process itself. Data that have been already migrated to a CSP are not further investigated by our proposed solution. In addition, it is also needed, to understand security needs of migrated data, so that authorities can adjust existing security policies, affecting the future information flow control.

Another question remaining refers to the implementation of our concept within an enterprise. In our evaluation we have asked only one employee of each participating enterprise to classify documents. However, it is absolutely necessary to involve more users of one enterprise in our conceptualized process in order to obtain significant training models that are linked with accurate security policies. At this point it needs to be explored, how existing CSP selection frameworks can interact with our proposed concept, ensuring that only trustworthy CSPs are allowed to process files with specific security levels.

With respect to our proposed security chain (cf. Figure 3) we have found that further research in using complex security policies is necessary. Then it should become possible to model dependencies between machine learning data and extracted metadata of documents.

VII. Conclusion

Machine learning is a fascinating research discipline that makes it possible to solve obscure and time consuming computing tasks. In this paper, we make use of machine mearning in order to provide cloud migration processes from the security point of view. We have presented a generic concept that enables authorities in enterprises to formulate security policies, controlling which types of data are allowed for migration to trustworthy cloud services. Therefore, we have introduced security levels within our concept that are building the link between document types and external CSPs.

In order to show that this concept is efficient we have developed a prototype that puts the ideas of our proposed concept into practise. Therefore, we assigned security policies to specific documents by using a naive Bayes classifier that automatically identifies particular document types. Users are deeply involved in our concept, as they can train the implemented classifier with real business documents and the related document types. In practice, employees do normally have the competence in their department to assign a document type to a certain file.

In the evaluation section we proved that our developed prototype is able to help users to determine whether a file is allowed for cloud migration or not in their daily business activities. In the case that a specific file

does not contain sensitive information, the user is shown visual information about possible CSPs, based on the designed security policies in the Cloud Data Inspector. The conducted laboratory experiment furthermore showed that our participants felt more secure when they were able to use a tool-based mechanism that helps them to decide which CSP is suited for processing specific files. As a consequence, our concept increases the users' trust in using external cloud services. Moreover, decision makers can be sure that a transparent and user centric process is used for cloud migration. On this basis we provide a fundamental contribution to the existing cloud adoption dilemma.

Taking everything into account, our work can be seen as a first step for further research activities in the problem context of cloud adoption and migration. We are convinced that data classification via machine learning is the key to support enterprises in security questions when it comes to data processing in cloud environments. However, our proposed concept and the supporting Cloud Data Inspector are not fully researched at this time. For example, our prototype is only able to process textual files so that is currently impossible to investigate binary files (i.e. zip-files). In addition, we need to find answers how CSPs can be evaluated and how it is possible to consider respective criteria in our proposed process. Another research question that is still open focuses on the quality of the machine learning algorithm. Therefore we have to run comprehensive quality tests in order to optimize the false positive rate. Finally, we want to investigate how our solution can be used on mobile devices.

References

[1] P. Mell and T. Grance, "The nist definition of cloud computing," 2011.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010. [Online]. Available: http://doi.acm.org/10.1145/1721654.1721672

[3] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Gener. Comput. Syst.*, vol. 25, no. 6, pp. 599–616, 2009.

[4] D. Truong, "How cloud computing enhances competitive advantages: A research model for small businesses," *The Business Review, Cambridge*, vol. 15, no. 1, pp. 59–65, 2010.

[5] T. C. Powell and A. Dent-Micallef, "Information technology as competitive advantage: The role of human, business, and technology resources," *Strategic management journal*, vol. 18, no. 5, pp. 375–405, 1997.

[6] P. Gupta, A. Seetharaman, and J. R. Raj, "The usage and adoption of cloud computing by small and medium businesses," *International Journal of Information Management*, vol. 33, no. 5, pp. 861–874, 2013.

[7] A. Khajeh-Hosseini, D. Greenwood, and I. Sommerville, "Cloud migration: A case study of migrating an enterprise it system to iaas," in *Proc. of the 3rd International Conference on Cloud Computing (CLOUD)*. IEEE, 2010, pp. 450–457.

[8] P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud migration research: A systematic review," *IEEE Transactions on Cloud Computing*, vol. 1, no. 2, pp. 142–157, 2013.

[9] T. Loruenser, A. Happe, and D. Slamanig, "Archistar: towards secure and robust cloud based data sharing," in *Proc. of the 7th International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE, 2015, pp. 371–378.

[10] P. Samarati and S. De Capitani di Vimercati, "Cloud security: Issues and concerns," *Encyclopedia on Cloud Computing. Wiley, New York*, 2016.

[11] S. Khanagha, H. Volberda, J. Sidhu, and I. Oshri, "Management innovation and adoption of emerging technologies: The case of cloud computing," *European Management Review*, vol. 10, no. 1, pp. 51–67, 2013. [Online]. Available: http://dx.doi.org/10.1111/emre.12004

[12] P. Srivastava, S. Singh, A. A. Pinto, S. Verma, V. K. Chaurasiya, and R. Gupta, "An architecture based on proactive model for security in cloud computing," in *Proc. of the International Conference on Recent Trends in Information Technology (ICRTIT)*, June 2011, pp. 661–666.

[13] BITKOM. (2015) Cloud-monitor 2015. [Online]. Available: https://www.bitkom.org/Publikationen/2015/Studien/Cloud-Monitor-2015/Cloud-Monitor-2015-KPMG-Bitkom-Research.pdf

[14] M. Diener, A. Kraus, and L. Fischer, "Einsatz von Cloud Computing in deutschen Unternehmen: Status quo und Bedeutung der Informationssicherheit," *Banking and Information Technology (BIT)*, vol. 17, no. 1, pp. 44–53, March 2016.

[15] R. H. von Alan, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS quarterly*, vol. 28, no. 1, pp. 75–105, 2004.

[16] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, 2007.

[17] J. Repschläger, R. Zarnekow, S. Wind, Turowski, and K. Turowski, "Cloud requirement framework: Requirements and evaluation criteria to adopt cloud solutions," in *Proc. of the 20th European Conference on Information Systems (ECIS)*, 2012.

[18] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.

[19] P. Samarati, "Data security and privacy in the cloud," in *Proc. of the 10th International Conference on Information Security Practise and Experience (ISPEC)*. Springer, 2014, pp. 28–41.

[20] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, "A survey on security issues and solutions at different layers of cloud computing," *The Journal of Supercomputing*, vol. 63, no. 2, pp. 561–592, 2012. [Online]. Available: http://dx.doi.org/10.1007/s11227-012-0831-5

[21] T. Lorünser, C. B. Rodriguez, D. Demirel, S. Fischer-Hübner, T. Groß, T. Länger, M. des Noes, H. C. Pöhls, B. Rozenberg, and D. Slamanig, "Towards a new paradigm for privacy and security in cloud services," in *Proc. of the 4th Cyber Security and Privacy EU Forum*. Sp, 2015, pp. 14–25.

[22] K. Ramachandran, H. Lutfiyya, and M. Perry, "On subjective trust for privacy policy enforcement in cloud computing," in *Proc. of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2013, pp. 1573–1580.

[23] T. Mather, S. Kumaraswamy, and S. Latif, *Cloud security and privacy: an enterprise perspective on risks and compliance*. O'Reilly Media, Inc., Sebastopol, Canada, 2009.

[24] A. López-Alt, E. Tromer, and V. Vaikuntanathan, "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption," in *Proc. of the 44th Annual ACM Symposium on Theory of Computing (STOC)*. ACM, 2012, pp. 1219–1234.

[25] M. Barbosa and P. Farshim, "Delegatable homomorphic encryption with applications to secure outsourcing of computation," in *Topics in Cryptology–CT-RSA 2012*. Springer, 2012, pp. 296–312.

[26] J. Wang, H. Ma, Q. Tang, J. Li, H. Zhu, S. Ma, and X. Chen, "Efficient verifiable fuzzy keyword search over encrypted data in cloud computing," *Computer Science and Information Systems*, vol. 10, no. 2, pp. 667–684, 2013.

[27] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, "Cryptdb: Processing queries on an encrypted database," *Commun. ACM*, vol. 55, no. 9, pp. 103–111, 2012.

[28] V. Ciriani, S. D. C. D. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Combining fragmentation and encryption to protect privacy in data storage," *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 3, 2010.

[29] M. Kunz, M. Hummer, L. Fuchs, M. Netter, and G. Pernul, "Analyzing recent trends in enterprise identity management," in *Proc. of the 25th International Workshop on Database and Expert Systems Applications (DEXA)*, 2014, pp. 273–277.

[30] S. D. C. Vimercati, S. Foresti, and P. Samarati, *Secure Cloud Computing*. Springer New York, 2014, ch. Selective and Fine-Grained Access to Data in the Cloud, pp. 123–148.

[31] B. Zwattendorfer, T. Zefferer, and K. Stranacher, "An overview of cloud identity management-models." in *Proc. of the 10th International Conference on Web Information Systems and Technologies (WEBIST)*, 2014, pp. 82–92.

[32] A. Sabouri and K. Rannenberg, "Abc4trust: protecting privacy in identity management by bringing privacy-abcs into real-life," in *Privacy and Identity Management for the Future Internet in the Age of Globalisation*. Springer, 2014, pp. 3–16.

[33] J. Zach and H. P. Reiser, "Livecloudinspector: Towards integrated iaas forensics in the cloud," in *Proc. of the 15th IFIP International Conference on Distributed Applications and Interoperable Systems (DAIS)*. Springer International Publishing, 2015, pp. 207–220.

[34] A. Fischer, T. Kittel, B. Kolosnjaji, T. Lengyel, W. Mandarawi, H. de Meer, T. Müller, M. Protsenko, H. Reiser, B. Taubmann, and E. Weishäupl, "Cloudidea: A malware defense architecture for cloud data centers," *Lecture Notes in Computer Science*, vol. 9415, pp. 594–611, 2015.

[35] A. Patel, M. Taghavi, K. Bakhtiyari, and J. C. Jnior, "An intrusion detection and prevention system in cloud computing: A systematic review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 25–41, 2013.

[36] S. Islam, E. R. Weippl, and K. Krombholz, "A decision framework model for migration into cloud: Business, application, security and privacy perspectives," in *Proc. of the 16th International Conference on Information Integration and Web-based Applications & Services (iiWAS)*. ACM, 2014, pp. 185–189.

[37] J. Repschläger, S. Wind, R. Zarnekow, and K. Turowski, "Decision model for selecting a cloud provider: A study of service model decision priorities," in *Proc. of the 19th Americas Conference on Information Systems (AMCIS)*, 2013.

[38] P. Saripalli and G. Pingali, "Madmac: Multiple attribute decision methodology for adoption of clouds," in *Proc. of the IEEE International Conference on Cloud Computing (CLOUD)*, 2011, pp. 316–323.

[39] A. Kanwal, R. Masood, U. E. Ghazia, M. A. Shibli, and A. G. Abbasi, "Assessment criteria for trust models in cloud computing," in *Proc. of the IEEE International Conference on Green Computing and Communications (GreenCom) and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing (iThings/CPSCom)*, 2013, pp. 254–261.

[40] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: Outsourcing computation without outsourcing control," in *Proc. of the ACM Workshop on Cloud Computing Security (CCSW)*. ACM, 2009, pp. 85–90.

[41] I. Kononenko and M. Kukar, *Machine Learning and Data Mining*. Woodhead Publishing, 2007.

[42] B. Pang, L. Lee, and S. Vaithyanathan, "Thumbs up?: Sentiment classification using machine learning techniques," in *Proc. of the ACL-02 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, vol. 10. Association for Computational Linguistics, 2002, pp. 79–86.

[43] F. Sebastiani, "Machine learning in automated text categorization," *ACM computing surveys (CSUR)*, vol. 34, no. 1, pp. 1–47, 2002.

[44] B. Liu, *Web Data Mining: Exploring Hyperlinks, Contents, and Usage Data (Data-Centric Systems and Applications)*. Springer, 2011.

[45] K. Siau and M. Rossi, "Evaluation techniques for systems analysis and design modelling methods a review and comparative analysis," *Information Systems Journal*, vol. 21, no. 3, pp. 249–268, 2011.

2 Herausforderungen für öffentliche Verwaltungen im Zeitalter von Cloud-, E-Government- und Smart-City-Projekten: ein kritischer Blick auf die Relevanz der Informationssicherheit

Publication details:

Status:	Published
Guest article in book:	Abschnitt 8.2: Herausforderungen für öffentliche Verwaltungen im Zeitalter der Digitalisierung: ein kritischer Blick auf die Relevanz der Informationssicherheit, (S. 208-223).
Date of submission:	January 22, 2022
Full citation:	MARKUS, H., 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*. Edition Innovative Verwaltung. Springer Gabler, Wiesbaden, pp. 205-242.
Authors' contributions:	Michael Diener 100%

Book series description: Die Bücher der Edition Innovative Verwaltung bieten praxisorientierte Fachinformation für Führungskräfte und Verantwortungsträger im öffentlichen Sektor. Die AutorInnen sind erfahrene PraktikerInnen aus der Kommunal-, Landes- und Bundes-Verwaltung sowie BeraterInnen und WissenschaftlerInnen. Sie teilen ihre Expertise, formulieren Empfehlungen, bieten Praxisleitfäden und geben Orientierung für eine erfolgreiche Öffentliche Verwaltung in der Zukunft. Das Themenspektrum spannt sich über die neuesten Herausforderungen in der Digitalen Verwaltung und Organisations- und Prozessthemen bis hin zu Führung und Leadership.

Titel

Herausforderungen für öffentliche Verwaltungen im Zeitalter von Cloud-, E-Government- und Smart-City-Projekten: ein kritischer Blick auf die Relevanz der Informationssicherheit

Einleitung

Der Ausbau der IT in öffentlichen Verwaltungen hat in den vergangenen Jahren schrittweise zu Veränderungen in der digitalen Kommunikation geführt. Die IT bildet heute die Grundlage moderner Verwaltungsabläufe – ohne sie, läuft nichts mehr. Und Digitalisierungsprojekte in den Bereichen E-Government, Smart-City, digitale Zwillinge etc. können nur dann erfolgreich sein, wenn die Informationssicherheit von Anfang an mitgedacht wird (vgl. Bostelmann 2021; BSI 2021, S.4). Umso wichtiger ist es, dass die IT zuverlässig und sicher betrieben wird. Besonders dann, wenn externe IT-Services aus der Cloud integriert werden. Hierfür braucht es aber gute und vor allem ausgereifte Konzepte sowie etablierte Sicherheitsmechanismen, die regelmäßig an die aktuellen Gegebenheiten angepasst werden. Damit ist nicht gemeint, dass nur Programmupdates und Anwenderprobleme fokussiert werden. Vielmehr zeichnet sich eine funktionierende IT-Sicherheitsorganisation dadurch aus, dass diese Chefsache ist (vgl. BSI 2021, S.66). Dies impliziert, dass zum einen alle Mitarbeitenden an dieser gewaltigen Aufgabe mitwirken. Zum anderen müssen Beschäftigte im IT-Bereich akribisch die Planung und Realisierung von Sicherheitsanforderungen unterstützen, damit etwaige Schwachstellen beseitigt sind, bevor diese von Cyberkriminellen ausgenutzt werden können.

Die jüngsten Medienberichte zeichnen jedoch ein anderes Bild, was die Lage der Informationssicherheit in einigen öffentlichen Verwaltungen und Behörden anbetrifft. Waren es vor ein paar Jahren noch wenige Ausnahmefälle über die berichtet wurde, häufen sich inzwischen fast wöchentlich die Nachrichten über Cyberangriffe, Datenpannen und lahmgelegte Institutionen (vgl. Tagesschau, 2021). In seinem jährlichen Lagebericht warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI) eindringlich vor

vielschichtigen Gefährdungen und Bedrohungen (vgl. BSI 2021, S.8-41) welche sich nicht nur auf Unternehmen, sondern auch auf die IT öffentlicher Verwaltungen auswirken können. Dass diese längst Realität wurden, zeigt der jüngste und prominenteste Fall am Beispiel des Landkreises Anhalt-Bitterfeld, der Anfang Juli 2021 von einer Cyberattacke schwer getroffen wurde (vgl. FAZ, 2021) und seitdem an der Lösung dieses massiven Sicherheitsvorfalls arbeitet. Abgesehen von dem Schaden, der sich aktuell auf mindestens 2 Mio. Euro beläuft, ist die Tatsache, dass Unberechtigte Zugriff auf sensible Daten der Verwaltung erlangten, nicht mehr rückgängig zu machen (vgl. Tremmel, 2021) – ein immenser Schaden für das öffentliche Ansehen der Verwaltung und ein Vertrauensverlust in die Sicherheit der Datenverarbeitung in Behörden.

Gleichzeitig sieht die Realität aber so aus, dass Cyberkriminelle immer raffiniertere Angriffsstrategien entwickeln, um ihre bösartigen Absichten zu verwirklichen, z. B. über sogenannte „Supply-Chain-Attacks", die das Eindringen in fremde Computersysteme mittels regulärer Software-Updates forcieren (vgl. Schmidt, 2021).

Insofern ist es wichtig, dass die grundlegendsten Aufgaben der Informationssicherheit in jeder öffentlichen Verwaltung umgesetzt werden. Zugleich braucht es eine aufgeschlossene Kultur gegenüber derartigen Herausforderungen, damit in Zukunft die Chancen der Digitalisierung im Behördenumfeld verwirklicht werden können. In diesem Buchbeitrag werden exemplarisch sieben ausgewählte Themenbereiche der Informationssicherheit betrachtet und vor dem Hintergrund praktischer Problemstellungen diskutiert. Dabei werden die Bereiche IT-Sicherheitsmanagement, Mitarbeitersensibilisierung, Sicherheitsupdates, Notfallvorsorgekonzepte, Risikomanagementprozesse, Schwachstellenscans und Cloud-Computing betrachtet.

1. Implementierung eines ISMS

Die Etablierung eines geeigneten Informationssicherheitsmanagementsystems (ISMS) in einer Organisation bildet die Grundlage, um flächendeckend, strukturiert und transparent die erforderlichen Sicherheitsprozesse dokumentieren und koordinieren zu können (vgl. Böhmer et al., 2017). In mittleren bis großen Verwaltungsbehörden haben sich in den letzten Jahren der BSI IT-Grundschutz (vgl. BSI, 2022a) sowie der ISO-Standard ISO 27001 (vgl. ISO, 2013) etabliert. Beide ISMS-Standards sind dafür geeignet, die komplexen Sicherheitsanforderungen in Behörden analysieren und verbessern zu können. Abbildung 1 skizziert den Umfang der betrachtenden Prozesse und IT-Systeme innerhalb des BSI IT-Grundschutzes. Für kleinere Organisationen sind diese beiden Standards im Regelfall aufgrund ihres Umfangs jedoch zu komplex. Aus diesem Grund wurde in den vergangenen Jahren der deutlich kompaktere ISMS-Standard CISIS12® (vgl. IT-Sicherheitscluster, 2022a) konzipiert, welcher Best-Practise-Ansätze aus ISO 27001 und Konzepte aus dem BSI IT-Grundschutz in vereinfachter Form verknüpft. Für Einsteiger lohnt sich ein Blick auf ISA+ (vgl. IT-Sicherheitscluster, 2022b) sowie auf das vom bayerischen Landesamt für Sicherheit in der Informationstechnik konzipierte Siegel „kommunale Sicherheit“ (vgl. LSI, 2022a). Auf Basis einfacher Fragekataloge kann eine Selbsteinschätzung zum Status der IT-Sicherheit in der betrachteten Organisation vorgenommen werden. Allen ISMS-Konzepten ist gemein, dass Verantwortliche für IT-Sicherheit sich kritisch mit den gegebenen IT-Strukturen auseinandersetzen müssen, um für diese geeignete Sicherheitsmaßnahmen ableiten zu können.

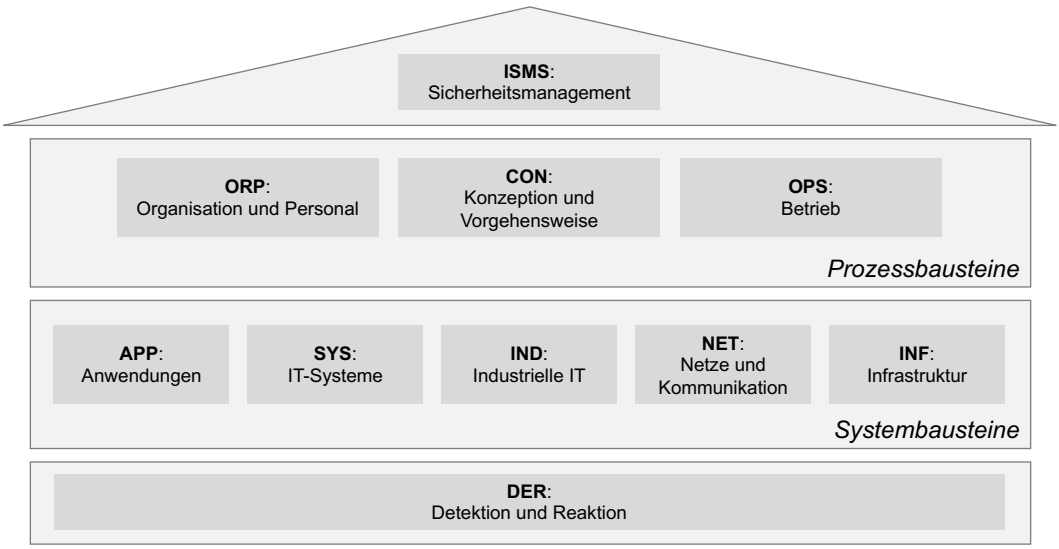


Abbildung 1: Bausteine des BSI-Schichtenmodells (Quelle: eigene Darstellung in Anlehnung an BSI 2022e, S.136)

Aktualität der IT-Dokumentation

Damit mit einem ISMS entsprechende IT-Sicherheitskonzepte entwickelt werden können, müssen zwingend in einem ersten Schritt alle IT-Komponenten (z. B. Anwendungsserver, Netzwerk, Firewall, Clients etc.) der Organisation strukturiert erfasst und dokumentiert werden. Hierbei sind u. a. Geschäftsprozesse und Infrastrukturen (z. B. Gebäude, Räume etc.) zu betrachten, in welchen sich die jeweiligen IT-Systeme befinden und auf denen die Datenverarbeitung stattfindet. Auch externe IT-Prozesse bei Cloud-Anbietern und Outsourcing-Partnern sind dabei einzubinden. Der Zeitaufwand für die Erstellung bzw. Aktualisierung einer IT-Dokumentation ist daher nicht zu unterschätzen, zumal mit steigender Größe der IT-Infrastruktur auch die Komplexität der Systemabhängigkeiten immens zunimmt. Damit dieses Vorhaben gelingen kann, sollte die Dokumentation von Beginn an mit einem geeigneten ISMS-Tool (vgl. Hofmann et al. 2017; aktueller: BSI 2022b) erfolgen.

Festlegung von Verantwortlichkeiten

Für die erfolgreiche Umsetzung von IT-Sicherheitsmaßnahmen ist es zwingend erforderlich, dass für jede dokumentierte Ressource (IT-Systeme, Anwendungsserver, Schnittstellen etc.) eine eindeutige Zuordnung der fachlichen Zuständigkeiten gegeben ist. Nur so lassen sich die in den IT-Sicherheitskonzepten enthaltenen Schutzmaßnahmen in der Praxis auch wirklich realisieren. Dementsprechend müssen die Verantwortlichen in Bezug auf die grundlegenden Konzepte eines ISMS qualifiziert werden, damit sie die damit einhergehenden Aufgaben bewältigen können, die für die Aufrechterhaltung der Sicherheitsmaßnahmen maßgeblich sind. Regelmäßig sind die Fortschritte zum Bearbeitungsstand der jeweiligen IT-Sicherheitsmaßnahmen zu evaluieren und dokumentieren, so dass frühzeitig bei eventuellen Abweichungen gegengesteuert werden kann.

2. Sensibilisierung des Personals für Informationssicherheit

Ein essenzieller Bestandteil des BSI IT-Grundschutzes fokussiert sich auf die Sensibilisierung des Personals, so dass ein sicherer Umgang mit IT-Ressourcen erreicht wird (vgl. IT-Grundschutz-Baustein ORP.3 in BSI 2022a). Im Fokus stehen in diesem Zusammenhang sogenannte Awareness-Schulungen. Darin werden u. a. die Grundlagen der Informationssicherheit den Bediensteten vermittelt (vgl. Weber et al. 2019a, S.9f.). Zielsetzung von solchen Schulungen ist es, alle IT-Nutzer*innen regelmäßig zu den wichtigsten IT-Sicherheitsvorgaben zu qualifizieren. Damit zählen Awareness-Schulungen zu den organisatorischen Maßnahmen, die ähnlich wie IT-Richtlinien, klare Regelungen für eine sichere Bedienung von IT-Systemen vorgeben. Beispielsweise sind Passwörter nur dann sicher, wenn dessen Besitzer*in sie auch sicher benutzen, diese also nicht außerhalb von Passwort-Safes aufbewahren.

Lernen und Trainieren mittels Security-Awareness-Tools

In größeren Organisationen empfiehlt sich der flächendeckende Roll-out von E-Learning-Tools zur online-basierten Durchführung von Awareness-Schulungen. Webbasierte Security-Awareness-Trainings (vgl. Gartner, 2022) bieten in der Regel vielseitige Interaktionsmöglichkeiten mit dem User, z. B. Erklär- und Lernvideos, Checklisten, interaktive Infotexte in Grafiken, Übungsaufgaben etc. Die Lerninhalte zu bestimmten Themen sind in einzelne Module strukturiert und werden meist mit einem Test abgeschlossen. Damit lässt sich der individuelle Lernfortschritt der Teilnehmer*innen dokumentieren. Integrierte Cockpits und Berichte liefern umfangreiche Statistiken über den organisationsweiten Fortschritt der Awareness-Kampagnen (vgl. Abbildung 2). Zudem lässt sich in E-Learning-Plattformen einstellen, welche Module bestanden sein müssen, ehe neue Teile des Security-Awareness-Trainings begonnen werden können. Viele Tools unterstützen die Bereitstellung digitaler Teilnahmezertifikate, so dass die Durchführung der Qualifizierungsmaßnahme nahezu vollautomatisch erfolgen kann.

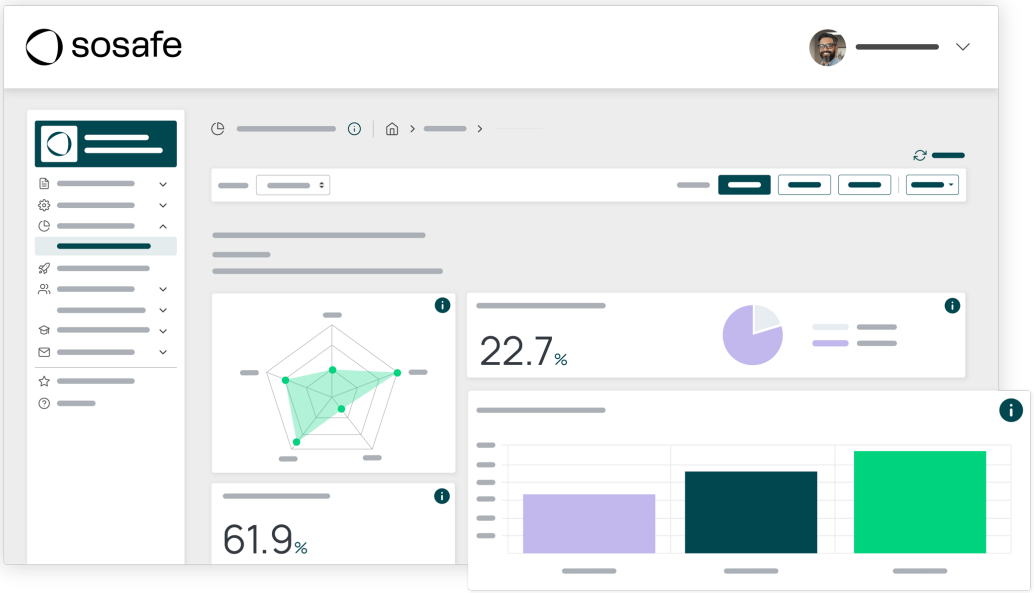


Abbildung 2: Management-Cockpit in einem Online-Awareness-Tool (Quelle: Sosafe 2022).

Laufende Wissensvermittlung

Eine kontinuierliche Vermittlung von Basiswissen zur IT-Sicherheit mittels unterschiedlicher Medien ist heute unerlässlich. Einerseits, um zügig auf aktuelle Gefahren und Bedrohungen reagieren zu können und andererseits deswegen, damit bereits vermitteltes Wissen weiterhin präsent bleibt. Es genügt nicht, dass eine zeitintensive Grundschulung zur IT-Sicherheit einmalig durchgeführt wird. Das Verhalten von Angreifern ändert sich, ebenso die realisierten Maschen und Tricks. Gerade was Angriffe mittels Social-Engineering-Techniken (vgl. Weber et al. 2019b, S.6f.) angeht, sind die Möglichkeiten für Cyber-Kriminelle nahezu grenzenlos. Es kommt dabei auf die Kreativität des einzelnen Angriffs an. Durch die Kombination verschiedener Angriffsstrategien gelingt es Angreifern immer wieder, Organisationen zu schaden. Daher muss Organisationsverantwortlichen klar sein, dass die beste IT-Firewall allein nicht ausreicht, wenn der eigentliche Angriff die zentrale Firewall umgeht und direkt die Menschen vor den Bildschirmen bedroht. Regelmäßige Wissensbeiträge auf unterschiedlichen Kanälen z. B. im Intranet, E-Mail-Newsletter oder Mitarbeiterzeitschriften können dabei helfen, die Awareness der Bediensteten zu verbessern. Darüber hinaus unterstützen spezielle Werkzeuge dabei, den Scharfsinn von Mitarbeiter*innen laufend zu trainieren, z. B. durch den kontinuierlichen Versand von Test-Phishingmails, die automatisiert von Simulatoren erzeugt werden und mögliche Klickereignisse auswerten können (vgl. Franz et al. 2020, S.597-612). Gerade bei der Nutzung externer Cloud-Services ist das Wissen um die Manipulierbarkeit von Login-Eingabemasken von besonderer Relevanz.

3. Zuverlässige Backups und Notfallvorsorgekonzepte

In Zeiten von zunehmenden Cyberangriffen in Form von Ransomware-Attacken sind aktuelle und funktionstüchtige Backups eine existentielle Sicherheitsvorkehrung (vgl. Jung, 2022). Haben Cyberkriminelle die Daten auf Anwendungs- und Fileservern erst einmal verschlüsselt, können diese ohne den passenden Schlüssel nicht wieder in den Ursprungszustand transformiert werden. In den meisten Fällen fordern Angreifer von den Opfern

Lösegeldzahlungen mittels kryptografischer Währungen (vgl. T2informatik, 2021). Inwieweit die Betroffenen dann tatsächlich den Entschlüsselungsschlüssel nach einer Zahlung erhalten und ob dieser dann auch funktioniert, ist ungewiss. Insofern darf es erst gar nicht so weit kommen, dass sich Unberechtigte Zugriff auf sensible Verwaltungsdaten verschaffen können. Dementsprechend braucht es neben technischen Sicherheitsmaßnahmen auch umfassende Datensicherungskonzepte (vgl. IT-Grundschutz-Baustein CON.3 in BSI 2022a), um genau solche Worst-Case-Szenarien zu verhindern.

Physisch getrennte und redundante Backups

In der Literatur wird im Kontext von Datensicherungen häufig auf die „3-2-1-Regel“ (vgl. Billo, 2018) verwiesen: mindestens 3 Datenkopien, mindestens 2 verschiedene Speichertypen und mindestens 1 Backup an einem externen Standort. Allerdings ist dieser Ansatz bei größeren Institutionen und vor dem Hintergrund des stetig wachsenden Datenvolumens heute ohne weiteres nicht mehr einfach umzusetzen. Mittlerweile stoßen klassische Bandsicherungen an ihre Grenzen, da die Dauer der Sicherungsvorgänge oftmals zu lange dauert und Daten sich zwischenzeitlich wieder verändert haben. Zur Lösung dieses Problems wird heute verstärkt auf Online-Backupstrategien gesetzt, bei der die zu sichernden Daten über das Netzwerk schnell auf andere Speichersysteme bzw. in externe Cloud-Storages übertragen werden (vgl. Rambadran, 2017). Was zunächst einfach und praktisch klingt, muss für den Einsatz im Tagesgeschäft gut geplant sein. In diesem Kontext sind u. a. Datenschutzanforderungen kritisch zu prüfen. Werden Backups in den eigenen Räumen aufbewahrt, ist grundsätzlich darauf zu achten, dass Datensicherungen und Produktivsysteme sich nicht im selben Brandabschnitt befinden. Eine räumliche Trennung zwischen Rechenzentrum und dem Ort, in welchem die Backups liegen, ist zwingend erforderlich (vgl. Standard-Anforderung CON.3.A12 in BSI 2022a). Idealerweise gibt es mindestens zwei voneinander unabhängige Räume, in welchen die Backups aufbewahrt werden (vgl. Abbildung 3). Natürlich darf hier nicht nur eine Version des Backups abgelegt sein, sondern

es braucht mehrere Versionen, die zu verschiedenen Zeitpunkten erzeugt wurden. Hintergrund ist der, dass eine Navigation in die Vergangenheit möglich sein muss, da bei zunächst unentdeckten Angriffen geklärt werden muss, welche Backup-Version frei von Schadsoftware ist. Darüber hinaus muss definiert werden, wie Zutritt, Zugang und Zugriff auf das Backup-System geregelt sind, so dass nur autorisiertes IT-Personal mit den gesicherten Datenbeständen in Berührung kommen kann.

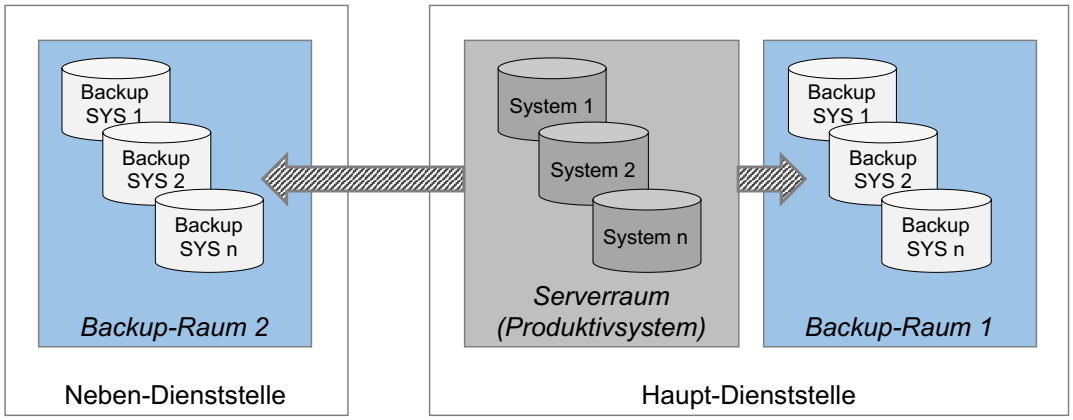


Abbildung 3: Räumlich getrennte Backups innerhalb der eigenen IT-Infrastruktur (Quelle: eigene Darstellung)

Aktualisierte Notfall- und Wiederanlaufpläne

Damit im Falle größerer IT-Störungen bzw. IT-Notfälle oder gar weitreichender Krisensituationen eine systematische Wiederinbetriebnahme der „kritischsten“ IT-Systeme, Anwendungen und Geschäftsprozesse realisierbar ist, sind umfangreiche Vorbereitungen für derartige Situationen mit einem Business Continuity Management (BCM) zu treffen. Das BSI hat hierzu den Standard 200-4 (vgl. BSI, 2022c) entwickelt. Im Wesentlichen verfolgt die Umsetzung eines BCM die Idee, systematisch Konzepte zu entwickeln und Organisationsstrukturen aufzubauen, die einen geregelten Notbetrieb zulassen und eine darauf aufbauende Überführung in den ursprünglichen Normalzustand unterstützen. Für Gemeinden, Märkte und kleinere Städte bietet das LSI Bayern eine weitere kompakte Hilfestellung mit dem „LSI IT-Notfallmanagement“ (vgl. LSI, 2022b) an.

4. Regelmäßige Sicherheitsupdates für IT-Systeme

Dem aktuellen Lagebericht des BSI zufolge hat die Anzahl neuer Varianten von Schadprogrammen im Vergleich zum Vorjahr um rund 144 Millionen zugenommen. Im Durchschnitt sind damit täglich mehr als 394.000 Varianten aufgetreten, was einem Anstieg von 22 Prozent entspricht (vgl. BSI 2021, S.11). Eine neue Variante entsteht aufgrund von Veränderungen im Quellcode einer Schadsoftware, wodurch deren Entdeckung deutlich schwieriger wird. Daher müssen IT-Systeme stets auf dem aktuellen Stand gehalten werden, insbesondere was Sicherheitsupdates anbetrifft. Abbildung 4 zeigt den im BSI-Lagebericht beschriebenen Trend im Kontext der zunehmenden Anzahl von Schadprogramm-Varianten.

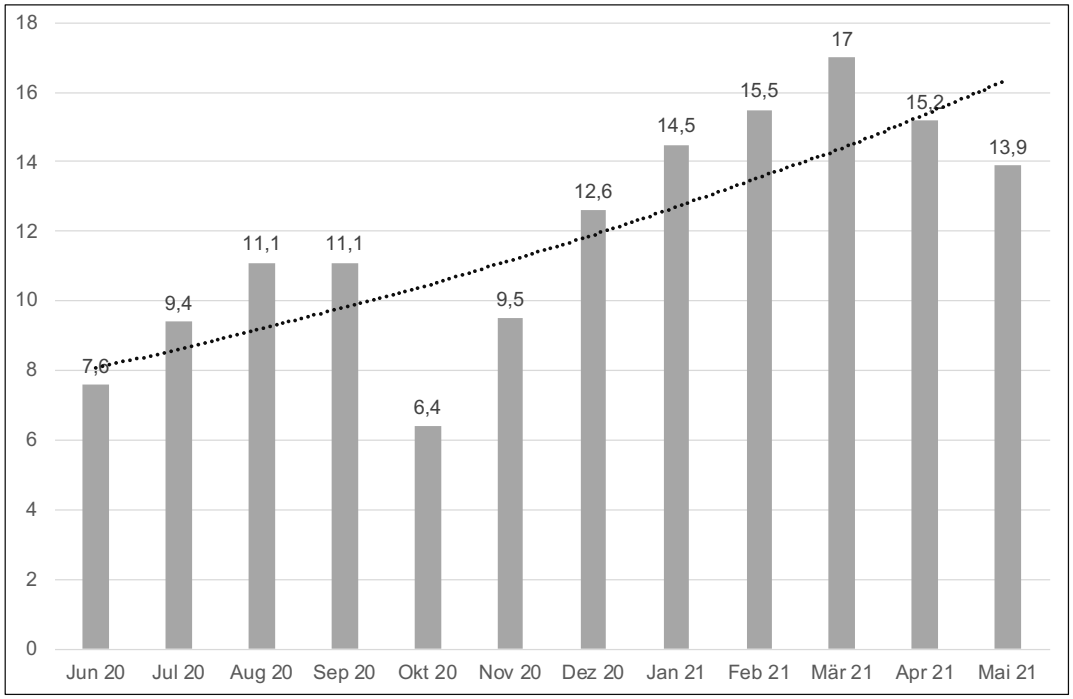


Abbildung 4: Entwicklung der Varianten von Schadprogrammen binnen eines Jahres (Quelle: eigene Darstellung in Anlehnung an BSI 2021, S. 11).

Infolge der zunehmenden Anzahl von IT-Komponenten steigt auch der personelle und zeitliche Aufwand, um zeitnah und zielgerichtet die Bereitstellung von Sicherheitsupdates für IT-Systeme zu organisieren (vgl. IT-Grundschutz-Baustein OPS.1.1.3 in BSI 2022a). Neben zentralen Netzwerkkomponenten (z. B. Router, Firewalls, Netzwerk-Switches, WLAN-

Controller) sind Windows- und Linux-Server sowie verschiedenste Endgeräte (z. B. Desktop-PC, Notebooks, Tablets, Smartphones etc.) regelmäßig mit Updates zu versorgen. Verstärkt kommen zukünftig auch netzwerkfähige Komponenten wie Drucker, IP-Videokameras, Türschließanlagen sowie Steuerungsmodule für Heizungs- und Klimaanlagen dazu. Darüber hinaus werden noch weitere Anbindungen von intelligenten Systemen, Sensoren und Aktoren bei IoT-Projekten (engl.: Internet-of-Things) erfolgen, welche insbesondere für Smart-City-Infrastrukturen relevant werden (vgl. Schäfer, 2021). Obwohl derartige Systeme auf dem ersten Blick zunächst wenig mit der klassischen IT einer öffentlichen Verwaltung zu tun haben, werden diese zukünftig mit städtischen Systemen vernetzt sein und erfordern deshalb entsprechende Sicherheitsupdates, damit eine Smart-City auch sicher funktioniert.

Tools vereinfachen die Softwareverteilung von Updates

Bereits in kleinen Organisationen ist eine zuverlässige Roll-out-Strategie von Sicherheitsupdates aufgrund der zuvor genannten Gerätevielfalt eine massive Herausforderung. Dementsprechend sind automatisierte Softwareverteilungen und Update-Installationen für diese verantwortungsvolle Aufgabe zielführend (vgl. Niemann 2013, S.206f.). Auf dem Markt werden hierfür verschiedene Softwareprodukte angeboten, die im Kontext des „IT-Service-Managements“ häufig eine Inventarisierung der Hard- und Software unterstützen und die zentrale IT-Dokumentation verknüpfen. (vgl. Haitz et al. 2019, S.74ff.). In jedem Fall ist ein toolgestützter Updatemechanismus insofern sinnvoll und notwendig, um stets den Überblick über den Fortschritt von Softwareupdates behalten zu können. Vor allem das Client-Management im Kontext von Home-Office stellt das IT-Personal vor weitere Herausforderungen, da Clients gegebenenfalls unregelmäßig mit den organisationsinternen Netzwerken verbunden sind, so dass die erfolgreiche Bereitstellung von Software-Aktualisierungen ein regelmäßiges Monitoring erfordert.

Zentrale Administration von Gruppenrichtlinien

Darüber hinaus spielen organisationsweite Sicherheitseinstellungen für Anwendungsserver und Clients eine maßgebliche Rolle in einem IT-Sicherheitskonzept. Gruppenrichtlinien ermöglichen eine feingranulare Konfiguration von Sicherheitsparametern, z. B. Einstellungen zur Passwortqualität oder deaktivierten bzw. eingeschränkten Features in Standardprogrammen (vgl. Joos et al. 2016). Um zu gewährleisten, dass Gruppenrichtlinien einheitlich und flächendeckend auf den betreffenden IT-Komponenten verteilt werden, muss deren Verwaltung über eine zentrale Management-Software bzw. einen Verzeichnisdienst erfolgen. Folglich lassen sich sehr schnell organisationsweite Anpassungen auf Servern und Clients durchsetzen, wobei jede Umsetzung einer Anpassung gut geplant sein muss. Vor diesem Hintergrund ist es ratsam, schrittweise die geplanten Änderungen auf die betreffenden IT-Systeme auszurollen. In jedem Fall sollten in einem ersten Schritt nur Geräte von technikaffinen Benutzer*innen einbezogen werden, damit diese etwaige Störungen oder Probleme melden können. Zudem ist die Dokumentation von zentralen Änderungen an Sicherheitseinstellungen von großer Bedeutung, so dass bei unerwarteten Problemstellungen die Suche nach möglichen Ursachen vereinfacht wird. Infolge der immer komplexer werdenden Abhängigkeiten von Gruppenrichtlinien sind Konflikte zwischen Usability und Security unvermeidbar. Sind diese nicht lösbar, liegen in der Regel Sicherheitslücken vor, die als potenzielle IT-Risiken zu behandeln sind.

5. IT-Risiken erkennen und behandeln

Sobald Anwendungen und Systeme in IT-Infrastrukturen betrieben werden, können diese vielschichtigen Gefährdungen (z. B. Brände, Stromausfälle, unberechtigter Datenzugriff etc.) ausgesetzt sein (vgl. BSI 2022e, S.152f.). In der Informationssicherheit stellen Gefährdungen von IT-Ressourcen potenzielle Sicherheitslücken bzw. IT-Risiken dar. Sobald ein IT-Risiko eintritt, werden IT-Leistungen nicht mehr wie erwartet erbracht (vgl. Seibold 2014, S.11). In der Regel wird durch den Eintritt einer Sicherheitslücke bzw. eines Risikos mindestens eines

der drei IT-Grundschutzziele verletzt, also die Vertraulichkeit, Verfügbarkeit oder Integrität der zu schützenden IT-Ressource.

Ein Risiko lässt sich gemäß BSI-Standard 200-3 für Risikomanagement (vgl. BSI 2022d, S.25f.) mit Hilfe von zwei Parametern näher definieren:

1) erwartete Häufigkeit des Eintretens eines schadhaften Ereignisses

2) potenzielle Höhe des Schadens im Falle eines Eintritts

Abhängig von der Ausprägung der beiden Parameter kann für ein Risiko eine entsprechende Risikokategorie (normal, mittel, hoch, sehr hoch) abgeleitet werden. In Abhängigkeit zur Kategorie der identifizierten Risiken muss eine Priorisierung der Bearbeitungsreihenfolge vorgenommen werden (vgl. Abbildung 5). In dem dargestellten Szenario würde zuerst Risiko 2 gefolgt von Risiko 1 behandelt werden müssen.

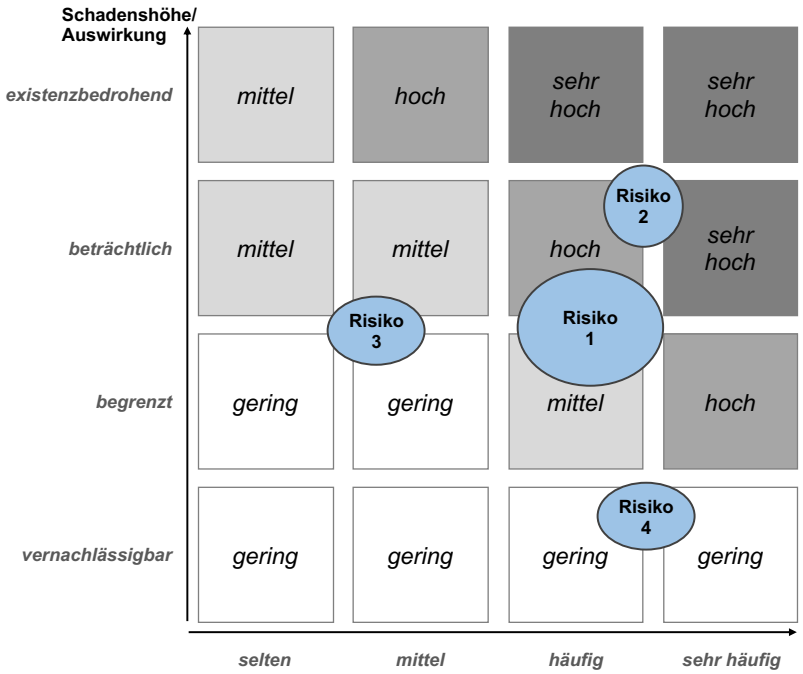


Abbildung 5: Priorisierung von Risiken nach Eintrittshäufigkeit und Schadenshöhe (Quelle: eigene Darstellung in Anlehnung an BSI 2022d, S.27)

Neben dieser Form der Risikodefinition existieren in der Literatur weitere Ansätze und Berechnungsmethoden. Allen ist gemein, dass abhängig von der Höhe respektive Kritikalität des bewerteten Risikos entsprechende Risikobehandlungsstrategien zu planen sind. Der BSI-Standard 200-3 kennt hierfür vier Ansätze (vgl. BSI 2022d, S.33f.):

- **Vermeidung** von Risiken: Ausschluss der Ursache eines Risikos
- **Reduktion** von Risiken: Anpassung der Eintrittshäufigkeit und/oder Schadenshöhe, um eine niedrigere Risikokategorie zu erzielen
- **Transfer** von Risiken: Überwälzung bzw. Teilung von Risiken mit anderen Organen, z. B. Versicherungen, externen IT-Dienstleistern etc.
- **Akzeptanz** von Risiken: Akzeptanz von bestehenden (Rest)-risiken, um die damit verknüpften Chancen realisieren zu können.

Etabliertes Risikomanagement

In der Praxis ist die Einrichtung eines Risikomanagementprozesses häufig mit weiteren Herausforderungen verbunden. Beispielsweise stellt sich bei komplexen Risiken meist die Frage nach den jeweiligen Zuständigkeiten. Beispielsweise sind Verantwortliche in Ämtern bzw. Abteilungen zu definieren, welche die Ausführung von administrativen und operativen Aufgaben im Kontext der gewählten Risikobehandlungsstrategie jeweils begleiten. Neben den personellen Ressourcen spielen die finanziellen Aspekte in diesem Zusammenhang eine entscheidende Rolle. Die Behandlung umfangreicherer Risiken erfordert deshalb u. a. die Bereitstellung ausreichend finanzieller Mittel, die zusätzlich neben den regulär anfallenden IT-Kosten aufzubringen sind. Darüber hinaus ist ein pragmatischer Ansatz für das Berichtswesen erforderlich, so dass die Leitungsorgane einer Behörde umfassend über die existierenden IT-Risiken und deren Status quo unterrichtet sind (vgl. Seibold 2014, S.214f.). Aus den genannten Gründen sollte die IT-Dokumentation für das ISMS mit dem Risikomanagementprozess unter Zuhilfenahme eines IT-Tools verzahnt werden.

6. Systematische Erkennung und Beseitigung von Sicherheitslücken

Gemäß den Einschätzungen des BSI stellt der Umgang mit Schwachstellen in IT-Infrastrukturen derzeit wohl eine der größten Herausforderungen für das Management der Informationssicherheit dar (vgl. BSI 2021, S.26 und S.87). In Ergänzung zu regelmäßigen Sicherheitsupdates muss neben einer sukzessiven Bearbeitung priorisierter Sicherheitslücken (vgl. Risikomanagementprozess) auch proaktiv nach Schwachstellen in der eigenen IT-Infrastruktur gesucht werden. Diese werden nach Bekanntwerden und sorgfältiger Recherchen über CERT-Portale (vgl. BSI 2022f) strukturiert kommuniziert (vgl. Abbildung 6). Allerdings beginnt mit jeder neuen Meldung für Systemverantwortliche die eigentliche Arbeit von vorne: alle relevanten IT-Systeme müssen daraufhin überprüft werden, inwieweit die Schwachstelle enthalten sein könnte.

Abbildung 6: CERT-Bund-Portal informiert über Schwachstellen und Sicherheitslücken in IT-Systemen (Quelle: Screenshot aus BSI 2022f).

Ein Wettlauf mit der Zeit beginnt, denn mit dem Bekanntwerden solcher Schwachstellen bereiten sich auch Cyberkriminelle mit „Hochdruck“ darauf vor, diese in schlecht gesicherten IT-Infrastrukturen auszunutzen. Dabei richtet sich ein Angriff möglicherweise nicht einmal gezielt gegen eine bestimmte Behörde oder Verwaltung: Angreifer setzen vielmehr darauf, Opfer aufgrund automatischer Scans zu finden. Die im Dezember 2021 gemeldete Schwachstelle zu „log4j“ (vgl. Beuth, 2021) wurde vom BSI zunächst mit dem Risiko „hoch“ klassifiziert (vgl. Abbildung 5), wenige Tage vor Weihnachten dann aber auf die Risikostufe „sehr hoch“ hochgestuft. Tatsächlich gelang es Cyberkriminellen über die log4j-Schwachstelle in Regierungsnetze einzudringen (vgl. Spiegel, 2021). Damit wird deutlich, dass derart existenzbedrohliche Schwachstellen in IT-Systemen so schnell wie möglich gefunden und beseitigt werden müssen. In der Praxis können bei solch anspruchsvollen Aufgabe spezielle Schwachstellenscanner oder externe Penetrationstests unterstützen.

Softwarebasierte Suche nach Schwachstellen

Mittels sogenannter Schwachstellenscanner (engl.: „Vulnerability Assessment Scanner“, kurz: VAS) ist es möglich, systematisch nach bekannten Mustern in IT-Systemen zu suchen. VAS-Tools müssen jedoch selbst kontinuierlich mit den neuesten Suchmustern aktualisiert werden, damit sie auch neuartige Sicherheitslücken identifizieren können (vgl. OWASP, 2022a). Auf dem Markt ist inzwischen eine große Auswahl an Schwachstellenscannern verfügbar. Sofern Muster in IT-Systemen identifiziert wurden, erfolgt eine Auflistung der Treffer in Sicherheitsberichten, abhängig von der Kritikalität der Schwachstelle. Ab diesem Zeitpunkt ist händische Arbeit nötig, für die qualifiziertes IT-Fachpersonal erforderlich ist. Schwachstellen müssen zunächst auf Plausibilität geprüft werden, denn „false-positives“ sind durchaus möglich. Bestätigt sich jedoch die Gültigkeit einer Schwachstelle in einer IT-Ressource, muss mit der Konzeption einer geeigneten Lösung für deren Absicherung begonnen werden. Abhängig von der jeweiligen Situation müssen gegebenenfalls IT-forensische Untersuchungen nach Beweisen eingeleitet werden, bei denen u. a. nach

sogenannten Kompromittierungsindikatoren (engl.: „Indicators of Compromise“, kurz: IoC) gesucht wird (vgl. Proofpoint, 2022). Damit ergeben sich für Verantwortliche von IT-Infrastrukturen weitere Herausforderungen, denn die Beseitigung und etwaige Untersuchung von Sicherheitslücken erfordern zusätzliche finanzielle und personelle Mittel – zusätzlich und unabhängig vom operativen IT-Betrieb. In jedem Fall müssen identifizierte Schwachstellen in den Risikomanagementprozess einfließen.

Externe Audits und Penetrationstests

Der Einsatz von VAS-Tools allein genügt jedoch nicht bei der Härtung und Absicherung von IT-Infrastrukturen, denn diese finden nicht unbedingt logische Sicherheitslücken. Das können beispielsweise Login-Formulare sein, die über das Internet erreichbar sind und keine Zwei-Faktor-Authentifizierung integriert haben. Derart problematische Designfehler in kritischen Sicherheitskomponenten lassen sich jedoch bei der Durchführung unabhängiger Penetrationstests aufspüren (vgl. Fox 2014, S.558). Abhängig vom festgelegten Untersuchungsgegenstand werden systematisch die erforderlichen Maßnahmen zur Absicherung der IT-Ressourcen auf ihre Wirksamkeit hin überprüft. Während bei einem Audit vor allem organisatorische Prozessabläufe untersucht werden (vgl. Gora 2009, S.238-246), liegt der Fokus bei Penetrationstests auf sicherheitstechnischen Einrichtungen. Beispielsweise wird u. a. geprüft, inwiefern es bei der Ausnutzung von Sicherheitslücken möglich ist, mittels SQL-Injections entsprechende Aktivitäten in Webanwendungen zu provozieren (vgl. OWASP, 2022b). Des Weiteren werden netzwerkspezifische Konfigurationen validiert, die beispielsweise LAN-Segmentierungen garantieren sollen. Interessant ist in diesem Zusammenhang, dass Behörden wie das Kraftfahrtbundesamt dazu übergehen, von Städten und Kommunen, die auf das Zentralregister zugreifen wollen, extern erstellte Nachweise über deren jeweils funktionierende Informationssicherheit einfordern (vgl. Bundesanzeiger, 2014).

7. Cloud-Computing in der öffentlichen Verwaltung

In den vergangenen Jahren haben sich auf dem Markt zahlreiche innovative IT-Lösungen etabliert, die zunehmend auf den Ideen und Konzepten des Cloud-Computings (vgl. Mell et al., 2011) beruhen. Im Wesentlichen lassen sich cloudbasierte IT-Services durch fünf zentrale Merkmale, drei Arten von Servicemodellen und vier unterschiedlichen Ansätzen für deren Bereitstellung klassifizieren (vgl. Abbildung 7). Vor allem die US-Unternehmen Amazon, Google und Microsoft haben massiv dazu beigetragen, dass das Paradigma des Cloud-Computings in der öffentlichen Wahrnehmung verständlicher und greifbarer wurde (vgl. Duta et al., 2019). So ist es binnen weniger Augenblicke möglich, einen vollwertigen Anwendungsserver mit zuvor festgelegten Parametern in Betrieb zu nehmen (vgl. Infrastructure-as-a-Service). Bezahlt wird nach der in Anspruch genommenen Rechenleistung, ohne dass hierzu ein physikalischer Server im eigenen Rechenzentrum notwendig ist. Zudem haben webbasierte Anwendungen als „Software-as-a-Service“ (kurz: SaaS) eine enorme Verbreitung erfahren und sind heute in vielen Organisationen fester Bestandteil der IT-Strategie. Beispielsweise ermöglicht SaaS eine cloudbasierte Zusammenarbeit mittels webbasierter Programmoberflächen und Datenspeichern, wodurch eine lokale Installation von Office-Produkten auf Clients vollständig entfallen kann. Dass heutige Cloud-Lösungen den Anforderungen einer hohen Nutzerfreundlichkeit und Flexibilität gerecht werden können, ist hinlänglich bewiesen. Gleichzeitig sind jedoch die damit einhergehenden Problemstellungen in Bezug auf den Datenschutz und die IT-Sicherheit weiterhin omnipräsent (vgl. Jäger et al. 2020). Einerseits ermöglicht der Einsatz cloudbasierter Technologien eine schnelle und kostengünstige Bereitstellung von IT-Dienstleistungen, andererseits müssen hingegen technische und organisatorische Maßnahmen ergriffen werden, um geltende gesetzliche Vorgaben wie die DSGVO einhalten zu können (vgl. Wissenschaftlicher Dienst, 2021).

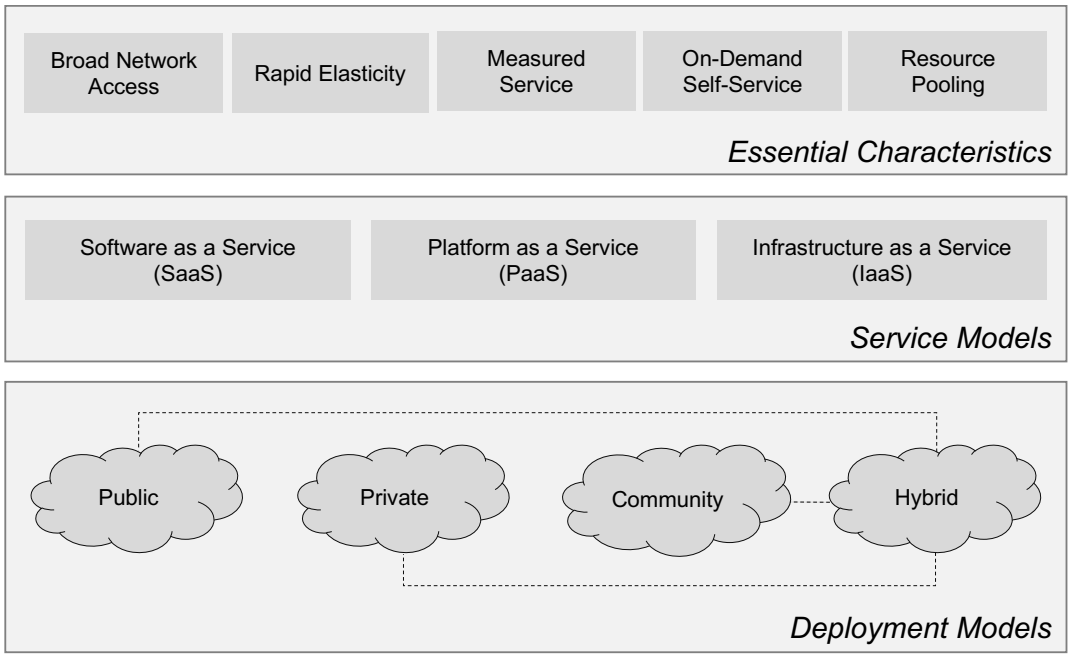


Abbildung 7: Eigenschaften von Cloud-Computing (Quelle: eigene Abbildung auf Basis von Mell et al. 2011).

Sichere Integration von Cloud-Services

Der Einsatz von IaaS-, PaaS- bzw. SaaS-Technologien wird aus den zuvor genannten Gründen früher oder später auch in öffentlichen Verwaltungen verstärkt betrachtet werden müssen (vgl. Hentschel et al., 2018). Spätestens mit Beginn der Covid-19-Pandemie wurde der Berieb cloudbasierter Videokonferenztechnologien für den Unterricht an Schulen kontrovers diskutiert. Für kommunale Sachaufwandsträger hat sich jedoch die Bereitstellung von Videokonferenz- und Kollaborationslösungen an Schulen als schwierige Herausforderung erwiesen (vgl. Kuketz, 2021). Ebenso sind in öffentlichen Verwaltungen die Anforderungen an sichere und funktionierende IT-Lösungen gestiegen, um pandemiebedingte Tätigkeiten im Home-Office zu ermöglichen. Häufig finden sich derartige Lösungsansätze weniger in „On-Premises-Lösungen“, sondern vermehrt in SaaS-Anwendungen. Daher erscheint die Erarbeitung einer Cloud-Strategie in öffentlichen Verwaltungen als zweckdienlich, um die rechtlich möglichen Optionen als auch die organisatorischen Voraussetzungen zu bestimmten

Anwendungsfällen klar definieren zu können (vgl. Sunyaev et al. 2015, S.117-138). Bei der Erarbeitung derartiger Regelungen sind u. a. die Mitwirkung der Beauftragten für Datenschutz und Informationssicherheit unerlässlich. In Ergänzung zu Cloud-Strategien braucht es Konzepte und Frameworks für die Auswahl geeigneter Cloud-Anbieter (vgl. Repschlaeger et al., 2012) sowie technische Mechanismen, um regelmäßig die Vertrauenswürdigkeit von Cloud-Anbietern überprüfen zu können (vgl. Diener et al., 2016). In diesem Zusammenhang sind auch die vom BSI definierten Mindestanforderungen für sicheres Cloud-Computing auf Basis des C5-Kriterienkatalogs zu betrachten (vgl. BSI, 2022g) sowie der ISO-Standard 27017 (vgl. ISO, 2015) der Sicherheitsanforderungen im Kontext von Cloud-Services definiert. Für die Regelung der Verarbeitung von personenbezogenen Daten in Cloud-Infrastrukturen existiert der ISO-Standard 27018 (vgl. ISO, 2020). Damit wird deutlich, dass es gut geplante Konzepte für Cloud-Computing in Behörden braucht, bevor diese beschafft werden können. In Ergänzung zur Auswahl von sicheren und datenschutzkonformen Cloud-Lösungen muss auch die lückenlose Integration in bestehende IT-Landschaften mitberücksichtigt werden.

Zusammenfassung und Ausblick

Abschließend kann festgehalten werden, dass sich der sichere Betrieb einer IT-Infrastruktur, unabhängig ob diese klein oder groß ist, aus der Perspektive der Informationssicherheit inzwischen zu einer zeit- und kostenintensiven Managementaufgabe entwickelt hat. Zugleich zeigen die Ausführungen dieses Beitrags, dass zukünftig die Gewährleistung der Informationssicherheit in öffentlichen Verwaltungen noch wichtiger wird. Die Zahl der Angriffe wird weiter steigen, denn der Erfolg bisheriger Cyberangriffe zeigte, dass das eine oder andere Opfer dennoch bereit war zu bezahlen – ein lukratives und aussichtsreiches Geschäftsmodell für Kriminelle. Dabei spielt es keine Rolle, ob eine kleine oder große Verwaltung per Zufall auf die Masche von Cyberkriminellen hereinfällt. Der Schaden ist immens, nicht nur aus finanzieller Sicht.

Alles Gründe, um die derzeitigen und noch folgenden Cybergefahren auf oberster Leitungsebene zur absoluten Chefsache zu machen. Diese Managementaufgabe beginnt mit der Beauftragung von qualifizierten IT-Fachpersonal, um operativ auf Systemebene die in diesem Beitrag benannten Aufgaben umzusetzen – und zwar als laufende Daueraufgabe. Ein bisschen IT-Sicherheit reicht heute nicht mehr aus. Tagtäglich erscheinen neue Varianten von Schadsoftware. Diese gilt es mit geeigneten Tools und Prozessen zu erkennen und von der Organisation abzuwehren. Eine Daueraufgabe, zu dessen Bewerkstelligung auch regelmäßige IT-Fortbildungen unumgänglich sind.

Zugleich ist es erforderlich, ein funktionierendes Risikomanagement mit Berichtsfunktion in der Verwaltungsleitung zu installieren. Auf dieser Ebene müssen dann auch geeignete Risikobehandlungsstrategien für die größten Risiken diskutiert werden, so dass aufgrund der nötigen finanziellen und personellen Kapazitäten eine echte Chance auf Heilung besteht. Ein wichtiger Punkt ist dabei ein offener und regelmäßiger Informationsaustausch zwischen der Verwaltungs- und IT-Leitung sowie den Beauftragten für Informationssicherheit.

Aufgrund der zunehmenden Vernetzung kommunaler Rechenzentren mit dem Internet infolge von E-Government- und Smart-City-Projekten steigt auch die Bedrohungslage zunehmend an. Es reicht daher nicht mehr aus, Finanzmittel für die einmalige Umsetzung derartiger IT-Projekte bereitzustellen. Im Gegenteil: es müssen Projektbudgets für den laufenden Unterhalt eingeplant werden. Zukünftig wird ebenso der Bedarf an Cloud-Lösungen zunehmen, um innovative IT-Services anbieten zu können. Dafür braucht es aber geeignete Cloud-Strategien, die zunächst erarbeitet werden müssen, wenngleich die Geschwindigkeit und Häufigkeit bzgl. Anfragen zur Integration von Cloud-Services steigen dürfte.

Des Weiteren werden öffentliche Verwaltungen von IT-Systemen noch stärker abhängig werden. Deshalb braucht es umfassende Sicherheits- und Notfallkonzepte, die im Vorfeld entwickelt werden müssen. Nur so ist es im Falle von größeren IT-Störungen und Notfällen möglich, die richtigen Maßnahmen für den Wiederanlauf zu initiieren. Dazu zählen neben Audits und Penetrationstests auch „IT-Sicherheits-Übungen“ in denen analog zu „Feuerwehr-Übungen“ erprobt wird, wer, was, wie im Ernstfall in welcher Reihenfolge zu tun hat. Ohne solche Übungen wird es dauern, bis die Wiederinbetriebnahme von Systemen gelingt – oder eben nicht, wie der Fall im Landkreis Anhalt-Bitterfeld zeigt. Hinzu kommt, dass auf Ebene der Verwaltungsleitung erkannt wird, wo die „kritischen Prozesse“ der eigenen Behörde liegen. Diese sind zunächst zu identifizieren und geeignet abzusichern. Bei dieser Aufgabe hilft der Einsatz eines ISMS mit integrierter IT-Dokumentation und einem etablierten IT-Service-Management. Dieses Zusammenspiel wird umso wichtiger, sobald sich Teile einer Kommune (vgl. Energie-, Wasser- und Abwassermanagement, Verkehrsleittechnik, Gesundheitswesen etc.) zu „kritischen Infrastrukturen“ entwickeln. Spätestens dann müssen aufgrund des geltenden IT-Sicherheitsgesetzes enorme Kraftanstrengungen unternommen werden, um Systeme und Prozesse bestmöglich gegenüber schadhaften Verhalten und Cyberangriffen abzusichern.

Einen wichtigen Baustein in einem guten IT-Sicherheitskonzept bilden die eigenen Mitarbeiter*innen. Diese gilt es entsprechend zu sensibilisieren, so dass diese in der Lage sind, IT-Bedrohungen zu erkennen und angemessen abzuwehren. Um dieses Level erreichen zu können sind regelmäßige Sensibilisierungsschulungen und Sicherheitstrainings nötig. In Summe bilden organisatorische und technische Sicherheitsmaßnahmen sowie die Integration der Menschen, welche die IT bedienen, eine umfassende Firewall, um öffentliche Verwaltungen wirksam abzusichern. Natürlich zählen zur Informationssicherheit noch weitere Teilgebiete. Aber die erfolgreiche Umsetzung von den in diesem Beitrag erwähnten Teilbereichen hilft bereits, einen guten Schutzschirm für eine Behörde aufzuspannen.

Literatur

Billo, T. (2018). *Was ist die 3-2-1-Backup-Regel?* https://www.storage-insider.de/was-ist-die-3-2-1-backup-regel-a-782641. Storage-Insider. Zugegriffen: 15.01.2022.

Beuth, P. (2021). *Wie löscht man ein brennendes Internet? Log4j-Sicherheitslücke*. https://www.spiegel.de/netzwelt/web/log4j-sicherheitsluecke-wie-loescht-man-ein-brennendes-internet-a-27729847-8e28-4187-b4a2-468a45137fb4. Spiegel. Zugegriffen: 23.01.2021.

Bostelmann, L. (2021). *Die Bedeutung der Informations-und Cybersicherheit bei der Umsetzung des Onlinezugangsgesetzes–Digitalisierung ja, aber (rechts) sicher!*. In Handbuch Onlinezugangsgesetz (S. 165-197). Springer, Berlin, Heidelberg.

Böhmer, W., Haufe, K., Klipper, S., Lohre, T., Rumpel, R., Witt, B. C. (2017). *Managementsysteme für Informationssicherheit (ISMS) mit DIN EN ISO/IEC 27001 betreiben und verbessern*. Beuth Verlag.

BSI. (2021). *Die Lage der IT-Sicherheit in Deutschland 2021*. Bundesamt für Sicherheit in der Informationstechnik.

BSI. (2022a). *IT-Grundschutz: Informationssicherheit mit System.* https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html. Bundesamt für Sicherheit in der Informationstechnik. Zugegriffen: 20.01.2022.

BSI. (2022b). *Alternative IT-Grundschutz-Tools.* https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Alternative-IT-Grundschutztools/alternative-it-grundschutztools_node.html. Bundesamt für Sicherheit in der Informationstechnik. Zugegriffen: 18.01.2022.

BSI. (2022c). *BSI-Standard 200-4: Business Continuity Management - Community Draft.* https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html. Bundesamt für Sicherheit in der Informationstechnik. Zugegriffen: 20.01.2022.

BSI. (2022d). *BSI-Standard 200-3: Risikomanagement.* https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html. Bundesamt für Sicherheit in der Informationstechnik. Zugegriffen: 20.01.2022.

BSI. (2022e). *BSI-Standard 200-2: IT-Grundschutz-Methodik.* https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-2-IT-Grundschutz-Methodik/bsi-standard-200-2-it-grundschutz-methodik_node.html. Bundesamt für Sicherheit in der Informationstechnik. Zugegriffen: 20.01.2022.

BSI. (2022f). *Kurzinfo CB-K21 / 1264: Information zu Schwachstellen und Sicherheitslücken.* https://www.cert-bund.de/advisoryshort/CB-K21-1264. Bundesamt für Sicherheit in der Informationstechnik. Zugegriffen: 23.01.2022.

BSI. (2022g). *Kriterienkatalog Cloud Computing C5*. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html. Bundesamt für Sicherheit in der Informationstechnik. Zugegriffen: 23.01.2022.

Bundesanzeiger. (2014). *Kraftfahrt-Bundesamt: Bekanntmachung des Standards für Internetbasierte Fahrzeugzulassung (i-Kfz) – Mindest-Sicherheitsanforderungen an dezentrale Portale –Stand: 13. November 2014 Version 1.0.* https://bundesanzeiger.de/pub/publication/bPbJuxPPBmUrtj0EN8I?0. Bundesanzeiger Verlag. Zugegriffen: 23.01.2022.

Diener, M., Blessing, L., Rappel, N. (2016). *Tackling the cloud adoption dilemma-A user centric concept to control cloud migration processes by using machine learning technologies*. In: Proceedings of International Conference on Availability, Reliability and Security (ARES) (pp. 776-785). IEEE.

Dutta, P., Dutta, P. (2019). *Comparative study of cloud services offered by Amazon, Microsoft & Google*. In: International Journal of Trend in Scientific Research and Development, 3(3), 981-985.

FAZ. (2021). *Erster Cyber-Katastrophenfall in Deutschland: Landkreis liegt lahm.* https://www.faz.net/aktuell/wirtschaft/digitec/erster-cyber-katastrophenfall-in-deutschland-landkreis-liegt-lahm-17431739.html. Frankfurter Allgemeine Zeitung. Zugegriffen: 10.01.2022.

Fox, D. (2014). *Penetrationstest*. In: Datenschutz und Datensicherheit-DuD, 38(8).

Franz, A., Benlian, A. (2020). *Spear Phishing 2.0: Wie automatisierte Angriffe Organisationen vor neue Herausforderungen stellen*. In: HMD Praxis der Wirtschaftsinformatik, 57(3).

Gartner. (2022). *Security Awareness Computer-Based Training Reviews and Ratings.* https://www.gartner.com/reviews/market/security-awareness-computer-based-training. Gartner Research. Zugegriffen: 15.01.2022.

Gora, S. (2009). *Security audits*. In: Datenschutz und Datensicherheit-DuD, 33(4).

Haitz P., Ranninger F. (2019). *Die Qual der Wahl: Marktübersicht Service-Management-Plattformen*. In: iX Magazin (3/2019). Heise.

Hentschel R., Leyh C. (2018) C*loud Computing: Status quo, aktuelle Entwicklungen und Herausforderungen*. In: Reinheimer S. (eds) Cloud Computing. Edition HMD. Springer Vieweg, Wiesbaden.

Hofmann, M., Hofmann, A. (2017). *ISMS-Tools zur Unterstützung eines nativen ISMS gemäß ISO 27001*. BoD E-Short.

ISO. (2013). *ISO/IEC 27001:2013. Information technology - Security techniques -Information security management systems – Requirements*. ISO.

ISO. (2015). *ISO/IEC 27017:2015-12. Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. ISO.

ISO. (2020). *ISO/IEC 27018:2020-08. Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (ISO/IEC 27018:2019)*. ISO.

IT-Sicherheitscluster e. V. (2022a). *CISIS12®*. https://cisis12.de. Zugegriffen: 15.01.2022.

IT-Sicherheitscluster e. V. (2022b). *ISA+Informations-Sicherheits-Analyse*. https://www.it-sicherheitscluster.de/isa/. Zugegriffen: 15.01.2022.

Jäger H.A., Rieken R.O.G., Ernst E. (2020). *Herausforderung Datenschutz und Datensicherheit in der Cloud*. In: Manipulationssichere Cloud-Infrastrukturen. Springer Vieweg, Wiesbaden.

Joos T., Schmitz P. *Mit Gruppenrichtlinien die Windows-Sicherheit verbessern: Definition Gruppenrichtlinien.* https://www.security-insider.de/mit-gruppenrichtlinien-die-windows-sicherheit-verbessern-a-555910. Security-Insider. Zugegriffen: 23.01.2022.

Jung, J. (2021). *Backups gegen Ransomware*. https://www.zdnet.de/88396561/backups-gegen-ransomware. ZDnet. Zugegriffen: 15.01.2022.

Kuketz, M. (2021). *MS Teams an Schulen: Duldung läuft bald aus – Fehlende Datenschutzkonformität*. https://www.kuketz-blog.de/ms-teams-an-schulen-duldung-laeuft-bald-aus-fehlende-datenschutzkonformitaet. Kuketz IT-Security Blog. Zugegriffen: 20.01.2022.

LSI. (2022a). *Bayerisches Siegel „kommunale IT-Sicherheit“.* LSI. https://www.lsi.bayern.de/kommunen/siegel_kommunale_it_sicherheit/index.html. Bayerisches Landesamt für Sicherheit in der Informationstechnik. Zugegriffen: 15.01.2022.

LSI. (2022b). *IT-Notfallmanagement.* LSI. https://www.lsi.bayern.de/kommunen/it_notfallmanagement/index.html. Bayerisches Landesamt für Sicherheit in der Informationstechnik. Zugegriffen: 15.01.2022.

Mell, P., Grance, T. (2011). *The NIST definition of cloud computing*. National Institute of Standards and Technology.

Niemann, K. D. (2013). *Client/server-Architektur: Organisation und Methodik der Anwendungsentwicklung*. Vieweg+Teubner Verlag.

OWASP. (2022a). *Vulnerability Scanning Tools.* https://owasp.org/www-community/Vulnerability_Scanning_Tools. OWASP. Zugegriffen: 23.01.2022.

OWASP. (2022b). *OWASP Top Ten.* https://owasp.org/www-project-top-ten. OWASP. Zugegriffen: 23.01.2022.

Proofpoint. (2022). *Indicators of Compromise (IoC).* https://www.proofpoint.com/de/threat-reference/indicators-compromise. Proofpoint. Zugegriffen: 23.01.2022.

Rambadran, P. (2017). *Rechenzentrum: Infrastrukturen für das Cloud-Zeitalter*. In: Wirtschaftsinformatik & Management, 9(1), 56-63.

Repschlaeger, J., Zarnekow, R., Wind, S., Klaus, T. (2012). *Cloud requirement framework: Requirements and evaluation criteria to adopt cloud solutions*. In: Proceedings of European Conference on Information Systems.

Schäfer, S. (2021). *4 IoT Smart City Beispiele: So gestalten Stadtwerke die kommunale Zukunft*. https://partner.mvv.de/blog/4-iot-smart-city-beispiele-so-gestalten-stadtwerke-die-kommunale-zukunft. MVV Blog. Zugegriffen: 23.01.2022.

Schmidt, J. (2021, 6. Juli). *Kaseya VSA: Wie die Lieferketten-Angriffe abliefen und was sie für uns bedeuten.* https://www.heise.de/hintergrund/Kaseya-VSA-Wie-die-Lieferketten-Angriffe-abliefen-und-was-sie-fuer-uns-bedeuten-6129656.html. Heise. Zugegriffen: 15.01.2022.

Seibold, H. (2014). *IT-Risikomanagement*. De Gruyter.

Sosafe. (2022). *SoSafe in der Presse*. https://sosafe.de/presse. SoSafe. Zugegriffen: 20.01.2021.

Spiegel. (2021). *Belgisches Militär von Angriff über Sicherheitslücke Log4j betroffen: IT-Schwachstelle*. https://www.spiegel.de/netzwelt/web/log4j-schwachstelle-belgisches-militaer-von-angriff-ueber-sicherheitsluecke-betroffen-a-aaf2d48c-84e8-4839-8f0b-77a1c4031fdd. Spiegel. Zugegriffen: 23.01.2022.

Sunyaev, A., Lansing, J. (2015). *Gestaltungsmöglichkeiten des Cloud Computing in der Verwaltung. In Wolken über dem Rechtsstaat?*. Nomos Verlagsgesellschaft mbH & Co. KG.

T2informatik. (2021). *Ransomware.* https://t2informatik.de/wissen-kompakt/ransomware. t2informatik. Zugegriffen: 15.01.2022.

Tagesschau. (2021). *Mehr als 100 Behörden erpresst: Hacker verschlüsseln Daten.* https://www.tagesschau.de/investigativ/br-recherche/ransomware-103.html. Tagesschau. Zugegriffen: 15.01.2022.

Tremmel, M. (2021). *Rebuilding Landkreis Anhalt-Bitterfeld: Nach Ransomware-Katastrophe.* https://www.golem.de/news/nach-ransomware-katastrophe-rebuilding-landkreis-anhalt-bitterfeld-2112-162045.html. Golem. Zugegriffen: 15.01.2022.

Weber K., Schütz A.E., Fertig T. (2019a). *Information Security Awareness*. In: Grundlagen und Anwendung von Information Security Awareness. essentials. Springer Vieweg, Wiesbaden.

Weber K., Schütz A.E., Fertig T. (2019b). *Der Faktor Mensch in der Informationssicherheit*. In: Grundlagen und Anwendung von Information Security Awareness. essentials. Springer Vieweg, Wiesbaden.

Wissenschaftlicher Dienst, (2021). *DSGVO und Nutzung US-amerikanischer Cloud-Dienste*. https://www.bundestag.de/resource/blob/852984/692120a134f9e79999c6f4170a47859a/WD-3-102-21-pdf-data.pdf. Deutscher Bundestag. Zugegriffen: 21.01.2021.

3 Cloud certification to foster digital transformation management in public administrations

Publication details:

Status:	Under review
Journal:	Journal of Problems and Perspectives in Management
Date of submission:	February 10, 2024
Full citation:	DIENER, M., ROESSLE, F., ROESSLE, K. Cloud certification to foster digital transformation management in public administrations. Submitted to: *Journal of Problems and Perspectives in Management*.
Authors' contributions:	Michael Diener 60% Dr. Felix Rößle 20% Prof. Dr. Kathrin Rößle 20%

Journal description: The purpose of the journal is coverage of different aspects of management and governance, such as international organizations and communities' management, state and regional governance, company's management, etc. The key aspects of planning, organization, motivation and control in various areas and in different countries are subject of the journal's scope. The journal publishes articles, which are focused on existing and new methods, techniques and approaches in the field of management. It publishes contemporary and innovative researches, including theoretical and empirical research papers.

Cloud certification to foster digital transformation management in public administrations

Keywords:

Public cloud services, cloud computing, public management, cloud adoption, information security management, data protection, digital sovereignty, EUCS certification scheme, certificate comparison.

JEL Classification:

M15, L86, H83

Authors:

Michael Diener, CISO, University and City of Regensburg, Regensburg, Germany, michael.diener@ur.de

Felix Roessle, Dr., Allianz Partners and University of Applied Sciences Rosenheim, Munich, Germany, felix.roessle@th-rosenheim.de

Kathrin Roessle, Prof. Dr., Technical University of Applied Sciences Rosenheim, Rosenheim, Germany, kathrin.roessle@th-rosenheim.de

Abstract

Cloud computing is a promising paradigm for public administrations to adopt high-performance IT-services without operating own data centers. However, public administrations in Europe are currently struggling with the adoption of public cloud services and face more severe challenges in the management than companies due to special requirements regarding data protection and information security. Nowadays, certification of cloud services is one of the most promising methods in overcoming the current issues.

The purpose of this article is to identify and to compare relevant cloud certifications that can support decision-makers in adopting sufficient cloud service providers and cloud services. The results show that existing certificates for cloud service providers do not match the requirements of public administrations. The analyzed cloud certificates focus strongly on the information security management and only have a general look on data protection management. The missing focus on the special requirements of public administrations regarding geolocation of servers, the US CLOUD Act, and especially prevention of foreign state access of personally identifiable information is most critical for the use in public administrations. This analysis proposes a Federal Risk and Authorization Management Program (FedRAMP) equivalent certification process combined with a European cloud certification scheme (EUCS) especially designed for governmental institutions that could be the trigger to a successful and faster cloud implementation in the public administration sector in Europe. Furthermore, it would create attractive business opportunities for cloud providers, fostering the development of innovative applications and serving the strategic goal of data sovereignty.

Introduction

Cloud-based services have become a disruptive business model in our agile and fast-growing information society. It is a standard that databases, complex business processes, meshed hardware infrastructure or dynamic microservices are migrated into cloud environments. As a new paradigm, cloud computing offers infinite possibilities to construct innovative digital services (Lin and Chen, 2012).

The efficacy of today's highly connected business processes can't be imagined without deep-integrated IT services from ubiquitous cloud offerings, e.g., when using Cisco Webex for video conferences, Microsoft 365 for collaboration, Amazon Web Services for computational power or artificial intelligence wizards from Google. Ready-to-use cloud applications like tools for project management can be quickly launched for major organizations just by registering user accounts and providing payment credentials (Saraswat and Tripathi, 2020). Thus, the advantages of digital government and cloud computing become increasingly important for companies and of course, the public administration sector, as the adoption of cloud services is usually faster and more cost-effective than operating own data centers (Subramanian et al., 2021).

Despite the tremendous benefits, public administrations in Europe struggle with the adoption of cloud computing, facing more severe challenges than corporations (Agarwal and Agarwal, 2011, Abraham et al., 2020). It is mandatory for them to comply with European and national laws, especially with focus on data protection (Altorbaq et al., 2017). This is in particular relevant when processing personal identifiable information (PII) (Rios et al., 2019). Cloud certifications are an important tool when choosing suitable IT services. There are multiple certifications in the market to support decision makers in this complicated process. Nevertheless, there are still concerns regarding the test criteria and scope of certificates with regard to data protection requirements, amongst others.

Literature Review

In general, literature on secure usage of public cloud services in the public administration sector is scarce. Investigating the cloud usage, this article aims to increase knowledge about specific obstacles for public administrations in Europe and provide solutions on how to leverage the implementation of cloud services. In particular, the article intends to contribute to the scientific literature by examining the most comprehensive sample of cloud certificates and analyzing their characteristics with regard to the demand of public administrations when choosing a suitable cloud service. Therefore, there is a need to provide criteria and solutions for practical usage and legislation, choosing secure cloud services or cloud service providers (CSP) in the context of public administrations.

Cloud computing is a business model that allows on-demand access to a shared pool of computing resources (e.g., networks, web-based applications) with pay-per-use costs and access from every point in the world via the internet (Mell and Grance, 2011). There are many large and small providers who offer cloud services with various pay-per-use pricing models and performance characteristics in all kinds of application areas of high interest for public services (Seo et al., 2014, Piswanger and Strick, 2017). In general, the idea of cloud computing is based on four unique deployment models, three different service models, and five essential characteristics. Figure 1 provides an overview about these principles.

Figure 1 about here

In general, IT departments do not need to own, maintain, or run the cloud infrastructure, platform, or application by themselves. The components are managed by

third-party companies (Ouedraogo and Mouratidis, 2013). The main advantages for outsourcing to a public cloud is leveraging IT resources (economies of scale) which is lowering costs, offering the appearance of infinite computing resources on demand and eliminating up-front expenditures, amongst others (Armbrust et al., 2010, Avram, 2014). However, the benefits of cloud services are also accompanied by various challenges and risks. Practitioners list data breaches as the #1 cloud computing threat (Walker, 2016). There are challenges from the cloud computing adoption perspective, but the main challenge is arising, when it comes to processing personal data (see e.g., Maithili et al., 2018, Dillon et al., 2010, Chen and Zhao, 2012). Especially, processing personal identifiable information (PII) requires well-prepared concepts to guarantee regulations. This applies not only to the processing of personal data, but to all data for which confidentiality and integrity are important (Hon et al., 2011). Data security, especially in terms of personal data is an issue that is even more important in the public vs. the private sector (Caudle et al., 1991).

The global cloud market is a well-developed and fast-growing market, growing from 43.8 billion USD in 2010 to almost 400 billion USD in 2022 and is expected to growth further to almost 1 trillion USD in 2026 (Markets and Markets, 2021, (Gartner, 2021). In Europe, up to 75% of the companies are using paid cloud services with the Nordic countries having the highest penetration (Eurostat, 2021). Interestingly, the use does not depend on the share of the information and communication technology sector in the GDP, but on factors such as companies employing specialists (Machuga, 2020). The main business is in the consumer and private sector, whereas spendings in the public sector remain small (Sullivan, 2022).

However, digitalization of the public administration sector is a key target for the European Union. Nevertheless, practical implementation is lacking behind the goals.

Today, the dominant cloud computing model in the public administration sector is the Government Cloud (Zwattendorfer et al., 2013). Trying to better use the new IT solutions and technologies for the public administration sector and the government, numerous states have also started supporting electronic government initiatives. As an example, the 'Bundescloud' in Germany offers an exclusive access to data for all members of the federal administration (Bundesregierung, 2022). Further examples are the National Cloud in Poland or the national cloud strategy in France (Dataguidance, 2021, ICTMarketExperts, 2019).

The issue of the underdeveloped IT infrastructure in the governmental sector, especially when comparing it to other regions (see e.g., Shen et al., 2023 with the example of China), was also evident during the covid pandemic (Agostino et al., 2021), and for example, the German government plans to heavily invest in the digitalization (SPD et al., 2021). However, the migration of services into public clouds remains a process with high uncertainties, as governmental organizations face additional constraints. They are mostly focusing on complying with legislation, protecting the citizens but also facing a shortage of qualified IT developers and feelings of uncertainty, fear and impatience and resilience of the public administration employees (Kuiper et al., 2014, Fischer et al., 2023). When it comes to cloud computing, governments as a first step have to build and align the national legislation with the one set by the European Union. Second, data security is an even more important factor in the public sector and third, different rules apply or the rules are followed by a stricter manner such as the US CLOUD Act or the requirement of having a data-center in Europe (Zaharia-Rădulescu and Radu, 2017, Rojszczak, 2020).

Especially the US CLOUD Act that enables US governmental authorities to get access to data stored outside the US, amongst others, is a challenge for all public cloud offerings (Abraha, 2019). It is in contrast to all data protection requirements in the EU

(Rutherford, 2019, Schwartz and Peifer, 2019). Therefore, a public administration planning to use a public cloud services has to contractually assure and check, whether the data will be processed at locations in line with legislation. To do so, the institution must perform data categorization and risk analysis and taking into account the possible risk of foreign state access (e.g., by intelligence or investigative agencies) (BSI, 2021). Unlike private organizations, the public administration cannot get permission from the customers via terms and conditions. Currently, the US CLOUD Act is restricting the public administration sector in Europe working with cloud offerings from US companies, when PII or even more critical data are involved.

Procuring information systems in the public administration sector is causing a dilemma. On the one hand, public administrations want to use the systems that meet their demands the best, but at the same time they are constrained by strict regulations (e.g., GDPR, US CLOUD Act) that limit the choice. This makes it difficult to outsource parts or entire IT processes to cloud environments. The limits (e.g., limited interaction possibilities with vendors due to tendering requirements) in the public administration sector are higher than those of private companies, and as research shows for private companies, there is an additional huge impact coming from technological readiness and digital immaturity at the local level of government (Moe et al., 2017, Gangwar et al., 2015, Kuhlmann and Heuberger, 2023, Margetts and Willcocks, 1993).

Usually, the process of outsourcing to a cloud is first executing the decision of the outsourcing itself, second the pre-selection of possible CSPs and third the final selection (Moe et al., 2017). In the beginning, customers make the general decision about outsourcing IT processes to the cloud. In that process, it is important to have customer involvement (see e.g., Dewarani and Alversia, 2023). Often, the choices for specific digital technologies are made by third parties (e.g., ICT departments of a city), rather than

by the users (Lember et al., 2019). The factors habit, cost and simplification have a special influence on the decision-making process (Benlian and Hess, 2011).

In step two, cloud service customers select providers based on a set of requirements or the offering that the customer is looking for. In most cases, only CSPs that offer the expected model and the required functions are considered (Garg et al., 2013). In the public administration sector, however, very often tenders are required to find the best provider. After the tender, the final selection for a service provider can be done based on the results of the tender.

In general, choosing the right CSP is a critical decision (Halabi and Bellaiche, 2017). There are various models helping the customers selecting the right offering. Most common are self-assessments, certificates or external audits (Tang and Liu, 2015).

When entering a business relationship with a CSP, there is a large set of uncertainty, especially regarding the trust of the provider (Lang et al., 2018). Trust is especially important, as it is also the primary influencing factor of the adoption of e-government (Janssen et al., 2021). Cloud service customers are looking for various controls and safeguards (Lang et al., 2016). Certification can play an important role in finding the right cloud solution, as buyers often lack specific knowledge and specifications are hard to check in a self-assessment (e.g., how is a small municipality supposed to check whether a non-European CSP meets the expected data protection requirements or not?).

Despite having a huge practical impact, purchasing cloud services and solutions in the area of public administrations is a neglected area of academic study. There are some studies tackling the general acquisition process of information systems. They show for example the dilemma between the idea of getting the system requirements right and strictly following regulations (Moe, 2014, Moe et al., 2017). Other publications mention

that specific certifications are required when providing cloud services to public sector organizations (Schneider and Sunyaev, 2014). Complexity and vender lock in are key issues regarding cloud adoption in public administrations (Ali et al., 2021, Opara-Martins et al., 2016). And in addition, specific stakeholders like politicians or domain specific regulations have an impact in public administration purchasing decision making (Schneider and Sunyaev, 2014).

When choosing a cloud service or provider, there is temporarily a huge lack of transparency (Sunyaev and Schneider, 2013). CSPs face many concerns from potential cloud service customers about trust in and security of the services they offer (Khan and Malluhi, 2013). To close this gap, customers could perform individual audits and perform self-assessments. In practice, it is common, that customers conduct on-site security and privacy audits before migrating their data into the cloud.

Nevertheless, it is often difficult to generate the trust into the offered cloud service and the provider itself. Therefore, certificates can help to foster trust between customers and providers, as they are extensively documenting the status of technical, organizational and legal matters, that are in most cases not visible for stakeholders outside cloud infrastructures (Lins et al., 2016, Lins et al., 2018).

A certification process usually encompasses an audit conducted by an independent and authorized third party that evaluates the cloud service and its organization. Overall, during an audit it is analyzed, how well the test criteria of the underlying certificate fit to the given situation at the cloud providers systems and processes. The most famous certification scheme that focuses on information security management is the ISO 27001.

Within the certification process it is problematic that once a certificate is granted, it usually has a validity period of one to three years. During this period, nonconformities

with the original audit might not be noticed, as providers confirm certification usually only during annual reviews (Krotsiani et al., 2015). However, this is still better than the alternative of each public administration performing a regular audit at each eligible CSP, showing the main advantage of cloud certificates.

Recent research in the field of cloud certification investigates technical approaches, that enable continuous monitoring of specific parameters (Lins et al., 2016, Lins et al., 2019). By applying this approach, transparent and actual reviews are possible. They support the buying public authorities by increasing their trust levels in ongoing audited cloud offerings.

Today, CSPs show various types of certificates on their websites and sales brochures. This increases the level of uncertainty regarding the evaluation criteria. When analyzing available cloud certificates and frameworks, it is obvious that there is no consistent method in the market (Gholami et al., 2016). This is even more critical when moving existing legacy systems to cloud platforms (Gholami et al., 2017). Despite various ambitions to create a market standard for cloud certifications, standards are developed independently, which is resulting in an incongruent and largely proprietary set of standards that varies in scope and underlying certification schemes and rule sets.

Summarized, there are several methods for static and dynamic certification of cloud services. Most of them are only available in literature. However, it is not clear to what extent decision makers, especially in local public administrations, have the necessary understanding of these cloud certifications. The purpose of our research is to systematically compare the different characteristics of the most important cloud certifications. In addition, the article investigates what changes or improvements need to be made to cloud service certifications in order to address information security and privacy concerns, particularly in the European public sector.

Method

Cloud certificates are the most promising method for leveraging cloud adoption in enterprises and public administrations. This article provides the most comprehensive sample of cloud certificates analyzed in the public administration sector so far. We solely consider cloud certificates targeting the European market or relevant to the European market, regardless of the primarily focus is on corporations or the public administration sector, as providers do not differentiate this factor. We do not consider UK certificates, as they no longer comply with the EU legal basis. We only use certificates that have practical evidence to public administrations. We don't consider minimum standards issued by government authorities as certificates, as they would require a self-evaluation and therefore lack the advantage of a certificate in leveraging cloud computing and we only consider standards available in English.

Moreover, we solely focus on certificates that are including major security topics like information security management. Thus, we ignore typical standards for quality management (i.e., ISO 9000), internal control mechanisms schemes (i.e., SOC 3, ISAE 3000), frameworks for governance (i.e., COBIT) or IT service management (i.e., ITIL, ISO 20000), amongst others. A very important factor in cloud certification is transparency of the underlying rule set. Therefore, we only investigate certificates that provide open access to the criteria catalogue. In addition, we do not consider cloud certificates focusing only on specific industries (e.g., PCI, TISAX, HIPAA, and HDS).

To put together the most comprehensive set of certificates, we extensively searched through various databases and the internet. First, we scanned databases (i.e., trusted-cloud) to identify certificates with European focus. To identify further missing certificates, we looked through publicly available lists on the internet, academic research, and did intensive research using common search engines. In addition, we reviewed cloud

certificates provided to large European cloud-service providers. Furthermore, we have interviewed more than 10 public administration experts (e.g., data protection officers) and investigated related practical and academic work, ongoing IT projects and information provided by public administrations creating a large knowledge base. Moreover, we analyzed in depth scientific cloud adoption frameworks, underlying jurisdiction, cloud certification guidelines and public private research projects. Finally, one author of this paper is Chief Information Security Officer (CISO) at a large public administration, which allows us to incorporate extensive practical expertise into this analysis. In total, we analyze 11 different cloud certificates.

Results

To analyze the most important characteristics of the cloud certifications for the public administration sector, we first identified the relevant dimensions. Based on the previously outlined method, we identified the following dimensions within the cloud certificates: (1) information security management, (2) risk management, (3) business continuity management, (4) documentation of sub service providers, (5) documentation of geo locations, (6) information processes due to official investigations, (7) the prevention of foreign state access and the (8) data protection management as the most critical factors for cloud certificates with regard to using them for cloud service adoption in the public administration sector.

Table 1 about here

Table 1 depicts the summary statistics of the cloud certificates. The table shows that most certification initiatives that are relevant for the public administration sector are somehow also driven by the public sector or by international associations such as the International Organization for Standardization (ISO). This demonstrates once again that

legislative has recognized the relevance and the problems and is searching for methods to solve the aforementioned challenges. Only the certificates of EuroPriSe, EuroCloud, EuroCloud Austria and CSA are provided by private or non-profit organizations. However, they have some relation to the public sector. The European Privacy Seal, for instance, was founded by a regional government in Germany and was supported by the European Union.

The advantage and need for certification of cloud computing is a subject that is already in discussion for quite some time. This is also shown by the launch dates of the certification initiatives, dating back to 1994. Nevertheless, the BSI IT-Grundschutz was not founded as a cloud relevant certificate, but developed over time with focus on information security management (ISM). Most of the certificates were introduced after 2010. The underlying rule set of a certificate is adjusted and updated from time to time. There are no standard cycles, also shown by the fact that some certificates are unchanged since 2015, obviously not taking into consideration any changes since then. The focus of the cloud certificates is mostly on data protection and information security, as these are the key issues regarding the security of a cloud, with 4 certificates having the focus on information security, 3 on data protection and 4 on both.

The certificate can be based on an underlying international and national standard or a criteria catalogue. The identified private organizations are usually based on European wide certification rules, whereas the ISO certificates are international standards and additional sub-specifications, such as the ISO 27017, which is a specific cloud service standard for providers. Target groups are in most cases the CSPs, who certify in order to prove that their offering is in line with the underlying guidelines of the certificate. On the buyer side, the IT-Organizations (ITOs) of cooperation's and public administrations are the other large target group.

The certificates are usually awarded to the CSPs after an extensive audit. The audit process getting the European Privacy Seal, for instance, has a comprehensive 6 step pre-check and evaluation, validation, and decision process prior to awarding the certificate. Audits can be performed by trusted third-parties (e.g., accredited auditors). Some of the providers perform the certification process in-house (e.g., the private European Privacy seal). Once a CSP has passed the certification process, the certificate is valid for several years.

The results of the 11 cloud certificates for the public administration sector are presented in table 2. The table illustrates the fulfilment grade of relevant characteristics for the use in the public administration sector.

Table 2 about here

Information security management (ISM) is an important dimension in all certificates. This criterion ensures that third-party audits or self-assessments have a close look in established and well-documented information security management processes. All certificates analyze this factor as a must have, however, with a different approach. For example, the ISO standards investigate the compliance of ISM systems in a more general view, which stands in contrast to the investigated principles in criteria catalogues. Certificates like the Cloud Security Alliance (CSA) STAR certificate, based on the underlying Cloud Control Matrix (CMM) evaluate the implementation of established and documented processes of information security management by various boolean (binary variable) questions.

The dimension risk management focuses on the management processes dealing with risk identification, its evaluation, treatment, and monitoring. Especially in cloud environments, risk management plays an important role with respect to the reduction or

elimination of security risks. This is a very important, but on the other hand very obvious topic in the criteria and controlled by all certificates. The ISO standards 27017 and 27018 do not check it on a must-have basis, however, as the ISO 27001 is a prerequisite of both sub-certificates, the existence of a risk management is still ensured.

Business continuity management (BCM) is describing the requirement of having a holistic approach aiming to prepare reaction plans and measurements in case of various types of incidents i.e., blackouts, system failures, cyber-attacks or fire alarms. Cloud customers expect a very high service level of the adopted cloud assets. 4 out of 11 cloud certificates do not expect BCM as a must-have criterion i.e., both sub-standards ISO 27017 and ISO 27018. Therefore, for cloud customers relying on this standard it is not defined what happens with their entrusted data and business processes in case of an incident. To tackle this problem, service level agreements (SLAs) need to be defined before adopting a cloud service.

The documentation of the involved sub-service providers of a cloud service is of key importance in the public administrations sector. It is already difficult to check the CSP, but it is even trickier to control the next levels. In practice, the cloud provider publishes a data processing agreement (DPA) which contains a full list of sub-contractors who are responsible for sub-processes within the offered cloud solution. This is significant for cloud customers, as they need to know all parties processing their data. Due to ongoing chances in the supply-chain, this is a complex factor in dynamic cloud infrastructures. For example, the simple integration of a database service operated at a third country like the United States or China can cause serious breaches with respect to data protection regulations. Recently, the usage of US-based web analytic tools was criticized in the context of GDPR by the national data protection authority of France. Well-established processes and rules in certificates can verify that CSPs make changes

transparent. Like in the BCM, the ISO 27017 and the ISO 27018 certificate do not insist on this. However, for the sub service provider documentation, also the ISO 27701 standard is not requiring information. All other certificates have sufficient documentation tested for a public administration.

Documented geo locations of cloud data centers, information processes caused by official investigations and the prevention of foreign state access all come from the same leading perspective, related to data protection and data sovereignty. Unauthorized access to governmental data, also by foreign states (e.g., United States, Russia, and China), intelligence or investigative agencies (e.g., NSA) must be prevented. Therefore, the geo location documentation is important, as public authorities need to make sure where their entrusted data is processed. 5 certificates only have should have rules. An example is the ISO 27001 standard, only defining very generally that sub-contractors should be listed. Therefore, such a certification cannot fully comply with the expectations of governmental institutions in the context of cloud adoption. The same applies to the BSI IT-Grundschutz that can only be obtained by conducting an ISO 27001 certification process.

Besides the possibility of an illegal access to data in the cloud, there might be legal access (e.g., after a judge has approved the access) by third parties. In such a case, an official investigation information process has to be in place to secure the interests of the cloud customer and the processed PII data. Our research provides insights, that ISO 27001 and BSI IT-Grundschutz do not obligatory force standardized information of cloud consumers or data owners in case of official investigations. However, this criterion is most important in context of European data protection regularities (cf. article 15 EU-GDPR). Therefore, a single use of this certificate is not sufficient for public administration. A combination with sub standards within the ISO 27000 family such as the ISO 27017 or ISO 27018 are required to guarantee to be in line with the statutes.

The inhibition of foreign state access to data is crucial for the governmental cloud activities. The provider shall only provide access or disclose data in the context of government investigation requests after a legal assessment or a court order. Unfortunately, this factor is only checked in 4 out of 11 certificates on a should have basis. Not a single certificate is providing this factor on a must have basis. This implies that this factor is of higher significance for governmental use than for private entities and is difficult to control. Neglecting this factor could lead to major violations of data security especially with regard to PII data and is not acceptable for public administrations.

Finally, we investigate at the data protection management perspective of the analyzed certificates. Only few test the data protection in the certificate itself, however, all others have a reference to national laws (e.g., GDPR) or other regulations that have to be fulfilled, allowing sufficient control for public administrations regarding the factor data protection.

The results in table 2 show that the certificates currently available are well designed to control the main risk factors related to a cloud. However, considering specific challenges for public administrations, the current offering is not sufficient to support leveraging cloud usage. None of the certificates available is supporting the public sector to all extents when choosing a cloud service. However, some certificates are at least able to help public administrations to choose the right service offering.

For example, the BSI C5 standard, which is amongst the most sophisticated standards of cloud security, would be sufficient for a public administration organization, if in addition, the prevention of foreign state access is guaranteed. This could be done by another check of the company providing the services to the public administration. The example of Amazon Web Services (AWS), one of the first cloud providers certified with the BSI C5 standard, shows the relevance of this additional check and underlines that the

existing criteria in the certification guidelines are not sufficient for public administrations. As a US company, AWS is also bound to follow US legislation and therefore committed to apply the rules of the US CLOUD Act (BSI, 2020). Moreover, a CSP using AWS or tools from any other US company or non-EU company is in almost every case not a suitable CSP for a public administration in Europe.

Looking at the fulfilment grade of the European Privacy Seal, this looks like an overall good fit for public administrations. Having a detailed look at the certified companies, however, it gets obvious that this certificate is not a good fit for the use in public administrations at this point in time. There are less than 20 companies certified and some of these companies don't even offer relevant services to public administrations (e.g., Lidl). Furthermore, the European Privacy Seal criteria are set by a private company. The company, EuroPriSe GmbH, issuing the certificate can adjust the rules. No matter what these adjustments are, it is very critical for public administrations to rely on a model without sufficient impact on the certification criteria.

Discussion

Using a cloud certificate checking most factors and doing additional checks for missing factors are one possible option to overcome the problematic for public administrations. However, this is still a complicated process and will most likely hinder the cloud from leveraging the full potential. Projects like Gaia-X, where business, science and politics are jointly developing the next generation of a European data infrastructure could be a well-suited solution for public administrations. Once available, new certificates could include Gaia-X compatibilities as a factor for public administrations. Though, this has a big disadvantage, as these certificates would only include a single technology or platform and would most likely exclude many innovative solutions.

Looking to other regions, there are more successful approaches in terms of leveraging the cloud in the public administration. For example, the US federal government is certifying cloud services with the Federal Risk and Authorization Management Program (FedRAMP) (FedRAMP, 2024). As of today, there are more than 330 authorized cloud services (for a full list, please refer to https://marketplace.fedramp.gov). This process significantly reduces duplicative efforts, inconsistencies, and cost inefficiencies on both sides, as public administrations do tests only once and also CSPs have an exact rule set. A set-up like FedRAMP is an aspirational target approach to enhance the adoption of secure and data protection compliant cloud computing for the public administration sector in Europe.

Table 3 about here

However, a set-up like FedRAMP requires a dedicated and fitting rule set for public administrations. There are several initiatives on European and governmental level targeting this gap in legislation. For instance, the French National Agency for the Security of Information Systems (ANSSI) developed requirements for CSPs (SecNumCloud) (ANSSI, 2022), guaranteeing that requirements for use in public administrations are met.

The Government Information Security Baseline (NEN, 2021), a standard of the Netherlands Standardization Institute (NEN) is enhancing the ISO 27001 requirements, targeting qualifications for offering cloud services for governmental institutions. The German federal government has even developed a minimum cloud standard for federal and state authorities (BSI, 2021), including very strict requirements, for instance regarding foreign state access. However, this cloud security standard is currently not mandatory for German municipalities. Finally, also the European Union is working on a certification scheme for all EU countries. The European Union Agency for Cybersecurity

(ENISA) is developing regulations for CSPs in the European Cybersecurity Certification Scheme for Cloud Services (EUCS) (ENISA, 2020). The current draft was mainly influenced by the BSI C5 and the France SecNumCloud requirements. Analyzing the described government rule sets with the same dimensions as in table 2, this could be a great leap forward for public administrations in Europe.

Table 3 presents the results and shows that the proposed guidelines are a significant step forward for public administrations cloud adoption in Europe. All four standards are controlling the most important topics for public administrations. Only BIO is lacking the must criteria for official investigation information process and prevention of foreign state access. Unfortunately, the BIO, BSI and SecNumCloud standards are all only available in the local language. In addition, for example, the SecNumCloud is cross-referencing to other PDF catalogues including additional French certification programs. Thus, the standard is not transparent for a use outside France. Positive is that at least some cloud providers already match the criteria of ANSSI (e.g., OVH Hosted Private Cloud).

To sum up, the EUCS approach, developing a version for Europe is the most important of the initiatives. The standard is fulfilling all requirements for public administrations and at the same time it is providing transparency and cross European usage. Combining this new set of rules with the US FedRAMP approach, this could significantly help the governmental sector in Europe to leverage cloud adoption. It would in addition provide a market with clear rules for solutions developed in environments like Gaia-X and companies being compliant with this set of regulation face a competitive advantage. It does not only overcome legal and technical issues, but also allows smaller public sector organizations to implement innovative cloud solutions. Nowadays, even federal and regional governments are struggling to implement cloud solutions; how should a small local administration be successful in the digital age?

With an official marketplace of pre-checked cloud solutions, a public administration would choose a service it is planning to implement, if needed make a tender inducing the requirement to have a FedRAMP equivalent certification process, and then implementing a state-of-the-art cloud service in line with all relevant European regulations.

The authors propose to additionally combine this approach with continuous dynamic cloud auditing, as the fast-changing supply chains require innovative solutions, and certificates can only be a confidence-building measure in the selection process, not a panacea for ongoing cloud security. As an interim solution, we propose a coordinated and simultaneous scheme for cloud services, which helps public administrations to independently conduct assessments and combine them with existing certificates, if necessary.

The solution to leverage cloud services in public administrations sounds simple, however, being compliant with the rule sets of BIO, EUCS, SecNumCloud or also the German federal government minimum cloud standard will be challenging for CSPs. Especially the US CLOUD Act in combination with European data security regulation is a powerful regulation, which requires significant IT knowledge and infrastructure in the European Union. Therefore, projects like Gaia-X are a prerequisite for a successful implementation of cloud services in the public administration sector. Otherwise, there is a legislation, but no cloud service being fulfilling the strict rule set.

The article proposes further research related to organizational and technical approaches in Gaia-X to construct suitable cloud certification processes for public administrations. In this context, it needs to be analyzed how the principles of FedRAMP can be integrated for a European marketplace that is administrated by an official European authority like ENISA. Moreover, the certification process needs to be transparent and

comprehensible regarding the criteria. In addition, the mechanisms of dynamic certification processes of cloud services should be analyzed. Meanwhile, this article proposes conducting further research in analyzing and designing a specific cloud requirement scheme that can be used temporarily by public administrations until the aforementioned Gaia-X solution is established.

Conclusion

The public administration sector is amongst the largest sectors in Europe. However, the adoption of public cloud services is weak and academic research is scant. This paper is the first evaluating how cloud certifications could help to develop the cloud adoption within the public administration sector.

The purpose of this research is to provide a systematic comparison of the major cloud certifications for use in the public administration sector, as they are key to leverage cloud offerings in the IT infrastructure of public administrations. The results show that each of the analyzed cloud certificates focuses strongly on the information security. In contrast, it becomes obvious that most certificates do only have a general look on data protection management. The missing focus on the special requirements of public administrations with regard to geo location of servers and especially prevention of foreign state access of PII data is most critical for the use in public administrations.

Concluding, there are several cloud certifications that use static methods. In the future, dynamic methods for cloud certification will play an increasingly important role in order to react flexibly to changes in information security and data protection. However, the results show that a Europe-wide regulation and methodology is needed to model the requirements of public administrations in a standardized way. In this context, the operation of a trusted cloud marketplace is seen as the best option to simplify and

accelerate the selection of CSPs for public administrations. The US FedRAMP model in combination with the EUCS certification scheme could serve as a model.

Author Contributions

Conceptualization: Michael Diener.

Data curation: Michael Diener.

Formal analysis: Michael Diener, Felix Roessle.

Investigation: Michael Diener, Felix Roessle

Methodology: Michael Diener.

Project administration: Michael Diener.

Supervision: Kathrin Roessle.

Validation: Felix Roessle, Michael Diener.

Visualization: Michael Diener.

Writing – original draft: Michael Diener, Felix Roessle, Kathrin Roessle.

Writing – review & editing: Michael Diener, Felix Roessle, Kathrin Roessle.

References

Abraha, H. (2019), How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis. International Data Privacy Law (3), 207–215. https://doi.org/10.1093/idpl/ipz009.

Abraham, A., Hörandner, F., Zefferer, T., & Zwattendorfer, B. (2020), E-government in the public cloud. Electronic Government, an International Journal (3), 260–280. https://doi.org/10.1504/EG.2020.108455.

Agarwal, A., & Agarwal, A. (2011), The security risks associated with cloud computing. International Journal of Computer Applications in Engineering Sciences, 257–259. https://doi.org/10.4236/vp.2020.64020.

Agostino, D., Arnaboldi, M., & Lema, M. (2021), New development: COVID-19 as an accelerator of digital transformation in public service delivery. Public Money & Management (1), 69–72. https://doi.org/10.1080/09540962.2020.1764206.

Ali, O., Shrestha, A., Ghasemaghaei, M., & Beydoun, G. (2021), Assessment of Complexity in Cloud Computing Adoption. Information Systems Frontiers, 1–23. https://doi.org/10.1007/S10796-021-10108-W/FIGURES/1.

Altorbaq, A., Blix, F., & Sörman, S. (2017), Data subject rights in the cloud. 12th International Conference for Internet Technology and Secured Transactions (1), 305–310. https://doi.org/10.23919/ICITST.2017.8356406.

ANSSI2022, Cloud computing service providers (SecNumCloud) requirements repository, Standard, Agence nationale de la sécurité des systèmes d'information (Paris, FR). Retrieved from https://www.cloud-temple.com/en/documentary-base/secnumcloud-standard-3-2.

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010), A view of cloud computing. Communications of the ACM (4), 50–58. https://doi.org/10.1145/1721654.1721672.

Avram, M.-G. (2014), Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. Procedia Technology (12), 529–534. https://doi.org/10.1016/J.PROTCY.2013.12.525.

Benlian, A., & Hess, T. (2011), Opportunities and risks of software-as-a-service. Decision Support Systems (1), 232–246. https://doi.org/10.1016/J.DSS.2011.07.007.

BSI2020, Cloud Computing Compliance Criteria Catalogue, Standard, Bundesamt für Sicherheit in der Informationstechnik (Bonn, DE). Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2020/C5_2020.html.

BSI2021, BSI minimum standard for usage of external cloud-services, Standard, Bundesamt für Sicherheit in der Informationstechnik (Bonn, DE). https://www.bsi.bund.de/dok/MST-Cloud.

Bundesregierung, I.-B. (2022), Bundescloud – an exclusive, private cloud for federal state organizations. Retrieved from https://www.itzbund.de/DE/itloesungen/egovernment/bundescloud/bundescloud.html.

Caudle, S., Gorr, W., & Newcomer, K. (1991), Key information systems management issues for the public sector. MIS Quarterly: Management Information Systems (2), 171–185. https://doi.org/10.2307/249378.

Chen, D., & Zhao, H. (2012), Data security and privacy protection issues in cloud computing. Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012, 647–651. https://doi.org/10.1109/ICCSEE.2012.193.

Dataguidance (2021), France Government announces national cloud strategy. Retrieved from https://www.dataguidance.com/news/france-government-announces-national-cloud-strategy.

Dewarani, G., & Alversia, Y. (2023), The influence of customer involvement and engagement on co-creation of services, satisfaction, and loyalty: The case of Software as a Service. Innovative Marketing (2), 27. https://doi.org/10.21511/im.19(2).2023.03.

Dillon, T., Wu, C., & Chang, E. (2010), Cloud computing. Proceedings - International Conference on Advanced Information Networking and Applications, AINA, 27–33. https://doi.org/10.1109/AINA.2010.187.

ENISA2020, European Union Cybersecurity Certification Scheme for Cloud Services, Standard, European Union Agency for Cybersecurity (Attki, GR).
Eurostat (2021), Percentage of companies with more than 10 employees in selected countries in Europe using paid cloud computing services.

FedRAMP (2024), Securing cloud services for the federal government. Retrieved from https://www.fedramp.gov/.

Fischer, C., Siegel, J., Proeller, I., & Drathschmidt, N. (2023), Resilience through digitalisation: How individual and organisational resources affect public employees working from home during the COVID-19 pandemic. Public Management Review (4), 808–835. https://doi.org/10.1080/14719037.2022.2037014.

Gangwar, H., Date, H., & Ramaswamy, R. (2015), Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. Journal of Enterprise Information Management (1), 107–130. https://doi.org/10.1108/JEIM-08-2013-0065/FULL/XML.

Garg, S., Versteeg, S., & Buyya, R. (2013), A framework for ranking of cloud computing services. Future Generation Computer Systems (4), 1012–1023. https://doi.org/10.1016/J.FUTURE.2012.06.006.

Gartner (2021), Cloud computing market research. Retrieved from https://www.gartner.com/.

Gholami, M., Daneshgar, F., Beydoun, G., & Rabhi, F. (2017), Challenges in migrating legacy software systems to the cloud — an empirical study. Information Systems, 100–113. https://doi.org/10.1016/J.IS.2017.03.008.

Gholami, M., Daneshgar, F., Low, G., & Beydoun, G. (2016), Cloud migration process—A survey, evaluation framework, and open challenges. Journal of Systems and Software, 31–69. https://doi.org/10.1016/J.JSS.2016.06.068.

Halabi, T., & Bellaiche, M. (2017), Evaluation and selection of Cloud security services based on Multi-Criteria Analysis MCA. 2017 International Conference on

Computing, Networking and Communications, ICNC 2017 , 706–710. https://doi.org/10.1109/ICCNC.2017.7876216.

Hon, W., Millard, C., & Walden, I. (2011), The problem of 'personal data' in cloud computing. International Data Privacy Law (4), 211–228. https://doi.org/10.1093/IDPL/IPR018.

ICTMarketExperts2019, Cooperation of the National Cloud Operator with Google Cloud. Retrieved from https://ictmarketexperts.com/en/news/cooperation-of-the-national-cloud-operator-with-google-cloud/.

Janssen, M., Rana, N., Slade, E., & Dwivedi, Y. (2021), Trustworthiness of digital government services: deriving a comprehensive theory through interpretive structural modelling. Digital Government and Public Management, 15–39. https://doi.org/10.1080/14719037.2017.1305689.

Khan, K., & Malluhi, Q. (2013), Trust in cloud services. Computer (7), 94–96. https://doi.org/10.1109/MC.2013.254.

Krotsiani, M., Spanoudakis, G., & Kloukinas, C. (2015), Monitoring-based certification of cloud service security. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 644–659. https://doi.org/10.1007/978-3-319-26148-5_44.

Kuhlmann, S., & Heuberger, M. (2023), Digital transformation going local: implementation, impacts and constraints from a German perspective. Public Money & Management (2), 147–155. https://doi.org/10.1080/09540962.2021.1939584.

Kuiper, E., van Dam, F., Reiter, A., & Janssen, M. (2014), Factors influencing the adoption of and business case for Cloud computing in the public sector. eChallenges 2014 - Conference Proceedings, 1–10.

Lang, M., Wiesche, M., & Krcmar, H. (2016), What are the most important criteria for cloud service provider selection? A Delphi study. European Conference on Information Systems, 1–17. Retrieved from https://aisel.aisnet.org/ecis2016_rp/119.

Lang, M., Wiesche, M., & Krcmar, H. (2018), Möglichkeiten zum Nachweis vertrauenswürdiger Cloud-Services. Management sicherer Cloud-Services, 59–68. https://doi.org/10.1007/978-3-658-19579-3_5.

Lember, V., Brandsen, T., & Tõnurist, P. (2019), The potential impacts of digital technologies on co-production and co-creation. Public Management Review (11), 1665–1686. https://doi.org/10.1080/14719037.2019.1619807.

Lin, A., & Chen, N.-C. (2012), Cloud computing as an innovation. International Journal of Information Management (6), 533–540. https://doi.org/10.1016/j.ijinfomgt.2012.04.001.

Lins, S., Grochol, P., Schneider, S., & Sunyaev, A. (2016), Dynamic Certification of Cloud Services. IEEE Security and Privacy (2), 66–71. https://doi.org/10.1109/MSP.2016.26.

Lins, S., Schneider, S., & Sunyaev, A. (2018), Trust is Good, Control is Better. IEEE Transactions on Cloud Computing (3), 890–903. https://doi.org/10.1109/TCC.2016.2522411.

Lins, S., Schneider, S., Szefer, J., Ibraheem, S., & 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 (44), 460–510. https://doi.org/10.17705/1CAIS.04425.

Machuga, R. (2020), Factors determining the use of cloud computing in enterprise management in the EU (considering the type of economic activity). Problems and Perspectives in Management (3), 93–105. https://doi.org/10.21511/ppm.18(3).2020.08.

Maithili, K., Vinoth-Kumar, L., & Latha, P. (2018), Analyzing the security mechanisms to prevent unauthorized access in cloud and network security. Journal of Computational and Theoretical Nanoscience (6-7), 2059–2063. https://doi.org/10.1166/JCTN.2018.7407.

Margetts, H., & Willcocks, L. (1993), Information technology in public services: disaster faster? Public Money & Management (2), 49–56. https://doi.org/10.1080/09540969309387763.

Markets and Markets (2021), Cloud Computing Market by Service Model (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)), Deployment Model (Public and Private), Organization Size, Vertical, and Region - Global Forecast to 2026. Retrieved from https://www.marketsandmarkets.com/.

Mell, P., & Grance, T. (2011), The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology (145), 1–7. Retrieved from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Moe, C. (2014), Research on Public Procurement of Information Systems. Communications of the Association for Information Systems (1), 78. https://doi.org/10.17705/1CAIS.03478.

Moe, C., Newman, M., & Sein, M. (2017), The public procurement of information systems. European Journal of Information Systems (2), 143–163. https://doi.org/10.1057/S41303-017-0035-4/TABLES/6.

NEN2021, Baseline Information Security Government, Standard, Stichting Koninklijk Nederlands Normalisatie Instituut (Delft, NL).

Opara-Martins, J., Sahandi, R., & Tian, F. (2016), Critical analysis of vendor lock-in and its impact on cloud computing migration. Journal of Cloud Computing (1), 1–18. https://doi.org/10.1186/S13677-016-0054-Z/FIGURES/11.

Ouedraogo, M., & Mouratidis, H. (2013), Selecting a Cloud Service Provider in the age of cybercrime. Computers & Security, 3–13. https://doi.org/10.1016/J.COSE.2013.01.007.

Piswanger, C.-M., & Strick, L. (2017), European innovation procurement “Pre-Commercial-Procurement” and Cloud computing by reference to the research project “Cloud for Europe”. 2017 Fourth International Conference on eDemocracy & eGovernment (ICEDEG) , 161–166. https://doi.org/10.1109/ICEDEG.2017.7962527.

Rios, E., Iturbe, E., Larrucea, X., Rak, M., Mallouli, W., Dominiak, J., Muntés, V., Matthews, P., & Gonzalez, L. (2019), Service level agreement-based GDPR

compliance and security assurance in (multi) cloud-based systems. IET Software (3), 213–222. https://doi.org/10.1049/iet-sen.2018.5293.

Rojszczak, M. (2020), CLOUD act agreements from an EU perspective. Computer Law & Security Review, 105442. https://doi.org/10.1016/J.CLSR.2020.105442.

Rutherford, M. (2019), The CLOUD Act. SSRN Electronic Journal . https://doi.org/10.2139/SSRN.3508942.

Saraswat, M., & Tripathi, R. (2020), Cloud Computing. 9th International Conference System Modeling and Advancement in Research Trends, 281–285. https://doi.org/10.1109/SMART50582.2020.9337100.

Schneider, S., & Sunyaev, A. (2014), Determinant factors of cloud-sourcing decisions. Journal of Information Technology (1), 1–31. https://doi.org/10.1057/JIT.2014.25.

Schwartz, P., & Peifer, K.-N. (2019), Data Localization Under the CLOUD Act and the GDPR. Computer Law Review International (1), 1–10. https://doi.org/10.9785/CRI-2019-200102.

Seo, J., Min, J.-S., & Lee, H. (2014), Implementation strategy for a public service based on cloud computing at the government. International Journal of Software Engineering and Its Applications (9), 207–220. https://doi.org/10.14257/ijseia.2014.8.9.17.

Shen, Y., Cheng, Y., & Yu, J. (2023), From recovery resilience to transformative resilience: How digital platforms reshape public service provision during and post COVID-19. Public Management Review (4), 710–733. https://doi.org/10.1080/14719037.2022.2033052.

SPD, Grünen, B., & FDP (2021), Mehr Fortschritt Wagen. Koalitionsvertrag.

Subramanian, G., Patil, B., & Gardas, B. (2021), Evaluation of enablers of cloud technology to boost industry 4.0 adoption in the manufacturing micro, small and medium enterprises. Journal of Modelling in Management, 944–962. https://doi.org/10.1108/JM2-08-2020-0207.

Sullivan, M. (2022), Public sector cloud adoption, Don't just adopt cloud computing, adapt to it. https://www2.deloitte.com/xe/en/insights/industry/public-sector/public-sector-cloud-adoption.html .

Sunyaev, A., & Schneider, S. (2013), Cloud services certification. Communications of the ACM (2), 33–36. https://doi.org/10.1145/2408776.2408789.

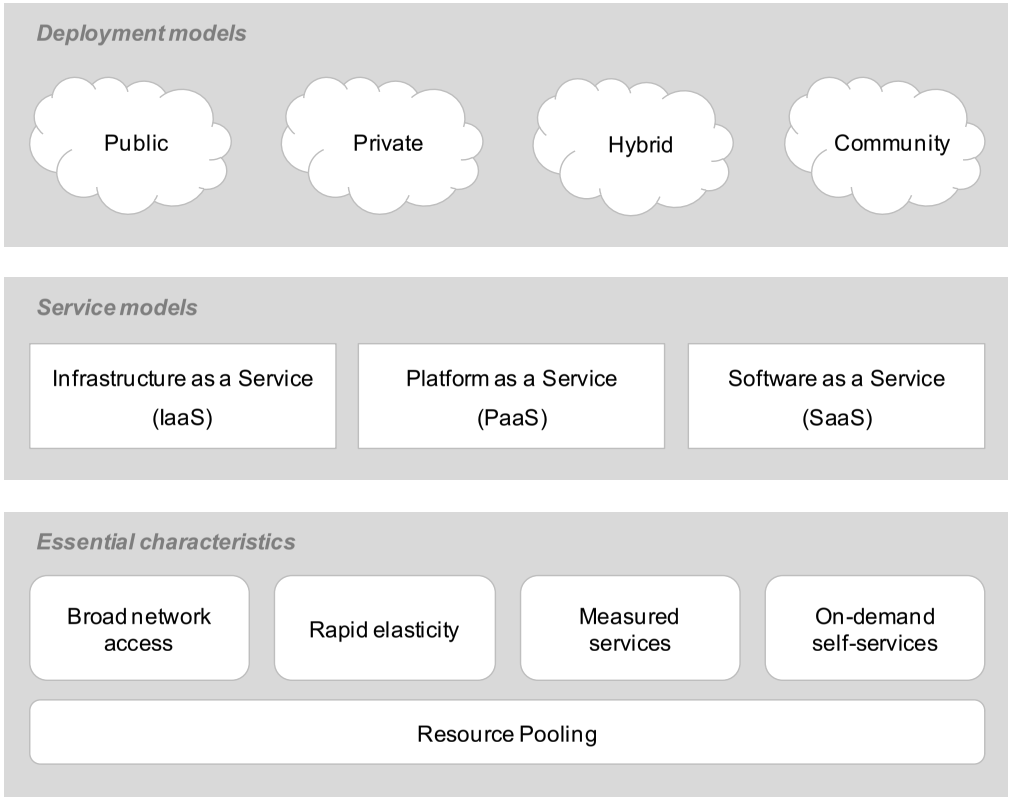
Tang, C., & Liu, J. (2015), Selecting a trusted cloud service provider for your SaaS program. Computers & Security, 60–73. https://doi.org/10.1016/J.COSE.2015.02.001.

Walker, K. (2016), CSA Releases Cloud Computing Top Threats in 2016. Retrieved from https://cloudsecurityalliance.org/press-releases/2016/02/29/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016.

Zaharia-Rădulescu, A.-M., & Radu, I. (2017), Cloud computing and public administration. Proceedings of the International Conference on Business Excellence (1), 739–749. https://doi.org/10.1515/picbe-2017-0078.

Zwattendorfer, B., Stranacher, K., Tauber, A., & Reichstädter, P. (2013), Cloud Computing in E-Government across Europe. Lecture Notes in Computer Science, 181–195. https://doi.org/10.1007/978-3-642-40160-2_15.

Figure 1. US National Institute of Standards and Technology definition of cloud computing



This figure presents the characteristics of cloud computing, split into deployment models, service models, and essential characteristics, as defined by the US National Institute of Standards and Technology.

Table 1. Summary statistics of cloud certificates

Certificate name	Provider	Provider organization type	Launch	Last Update	Main Focus	Type	Target group	Validity [years]
AUDITOR	Auditor Cert	Government supported	2019	Jan 20	DP	Criteria Catalogue	CSPs, ITOs	-
BSI C5	BSI	Government	2016	Feb 20	IS	National Standard (Germany)	CSPs	1
BSI IT-Grundschutz	BSI	Government	1994	Feb 22	IS	National Standard (Germany)	ITOs	3
CSA STAR	CSA	Non-profit	2010	Jul 21	DP, IS	Criteria Catalogue	CSPs, ITOs	3
EuroCloud StarAudit	EuroCloud	Non-profit	2009	Dez 20	DP, IS	Criteria Catalogue	CSPs, ITOs	3
European Privacy Seal	EuroPriSe	Private	2007	Jan 17	DP, IS	Criteria Catalogue	IT products and services	2
ISO 27001	ISO	International association	2005	Sep 13	IS	International Standard	ITOs	3
ISO 27017	ISO	International association	2015	Dez 15	IS	International Standard	CSPs, ITOs	3
ISO 27018	ISO	International association	2014	Jan 19	DP	International Standard	CSPs, ITOs	3
ISO 27701	ISO	International association	2019	Aug 19	DP	International Standard	CSPs, ITOs	3
Ö-Cloud-Gütesiegel	EuroCloud Austria	Non-profit	2021	Dez 20	DP, IS	Criteria Catalogue	CSPs, ITOs	1

This table presents the summary statistics on cloud certificates with influence on choosing a cloud for the public administration sector, including the name of the certificate, the name of the provider, the launch and last update of the guidelines and specifications of the underlying rule set of the certificate, the main focus (DP = Data Protection; IS = Information Security), the type, the main target group, and the validity of the certificate in years.

Table 2. Cloud certificates fulfilment grade for public administration requirements

Certificate name	ISM	RM	BCM	Sub service provider documentation	Geo location documentation	Official investigation information process	Prevention of foreign state access	Data protection management proceedings
AUDITOR	✓✓	✓✓	✓	✓✓	✓✓	✓✓	x	✓✓
BSI C5	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓	reference to national DP laws
BSI IT-Grundschutz	✓✓	✓✓	✓✓	✓✓	✓	x	x	reference to national DP laws
CSA STAR	✓✓	✓✓	✓✓	✓✓	✓✓	✓	x	reference to national DP laws, internal regulations
EuroCloud StarAudit	✓✓	✓✓	✓✓	✓✓	✓✓	✓	x	✓✓
European Privacy Seal	✓✓	✓✓	✓	✓✓	✓✓	✓✓	✓	✓✓
ISO 27001	✓✓	✓✓	✓✓	✓✓	✓	x	x	reference to national DP laws, internal regulations
ISO 27017	✓✓	✓	✓	✓	✓	✓	x	reference to national DP laws
ISO 27018	✓✓	✓	✓	✓	✓	✓	✓	reference to national DP laws
ISO 27701	✓✓	✓✓	✓✓	✓	✓	✓	✓	reference to national DP laws, internal regulations
Ö-Cloud-Gütesiegel	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	x	✓✓

This table presents the cloud certificates and the fulfilment grade of relevant characteristics for the use in the public administration sector, including the check of information security management (ISM), risk management (RM), business continuity management (BCM), sub service providers documentation, official investigations information process, prevention of foreign state access for example by intelligence or investigative agencies, and data protection management proceedings of the cloud certificate. “x” identifies not specified, “✓” identifies should-have or optional requirements in the underlying certification guidelines and “✓✓“ identifies must-have and obligatory requirements in the underlying certification guidelines.

Table 3. Governmental regulation initiatives for cloud services

Certificate name	ISM	RM	BCM	Sub service provider documentation	Geo location documentation	Official investigation information process	Prevention of foreign state access	Data protection management proceedings
BIO	✓✓	✓✓	✓✓	✓✓	✓✓	✓	✓	✓✓
BSI minimal cloud standard	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	ref. to national DP laws
EUCS	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	ref. to national DP laws
SecNumCloud	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓

This table presents governmental regulation initiatives for cloud services and the fulfilment grade of relevant characteristics for the use in the public administration sector, including the check of information security management (ISM), risk management (RM), business continuity management (BCM), sub service providers documentation, official investigations information process, prevention of foreign state access for example by intelligence or investigative agencies, and data protection management proceedings of the cloud certificate. “x” identifies not specified, “✓” identifies should-have or optional requirements in the underlying certification guidelines and “✓✓“ identifies must-have and obligatory requirements in the underlying certification guidelines.

4 Cloud Inspector: A tool-based approach for public administrations to establish information security processes towards public clouds

Publication details:

Status:	Published
Conference:	9th International Conference on Information Systems Security and Privacy, ICISSP 2023, Lisbon, Portugal, February 22 - 24, 2023
Date of acceptance:	November 11, 2022
Full citation:	DIENER, M., BOLZ, T. (2023). Cloud Inspector: A tool-based approach for public administrations to establish information security processes towards public clouds. In *Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP)*, Lisbon, Portugal, pp. 543-551.
Authors' contributions:	Michael Diener 90% Prof. Dr. Thomas Bolz 10%

Conference description: The International Conference on Information Systems Security and Privacy is an event where researchers and practitioners can meet and discuss state-of-the-art research about the technological, social, and regulatory challenges that regard the security, privacy, and trust of modern information systems. The conference welcomes papers of either practical or theoretical nature, and is interested in research or applications addressing all aspects of trust, security and privacy, and encompassing issues of concern for organizations, individuals and society at large.

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*
michael.diener@ur.de, thomas.bolz@iu.org

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 upfront 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).

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.

[1] https://fedramp.gov
[2] https://gaia-x.eu

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

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).

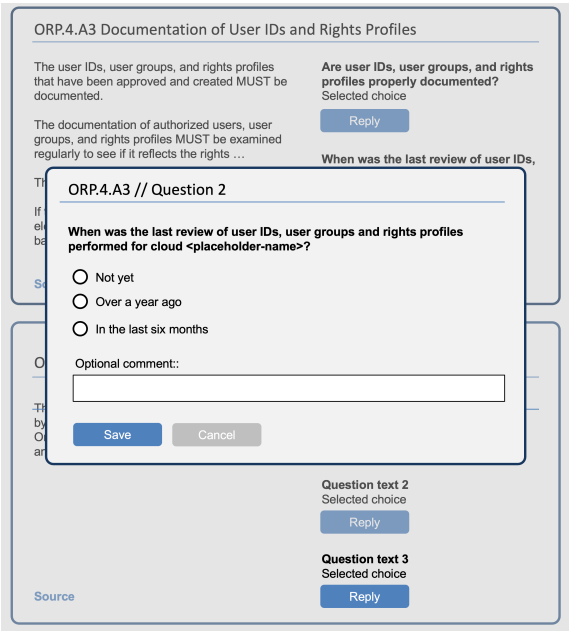


Figure 1: Proposed design for questionnaire

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 questionnaire.

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

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.

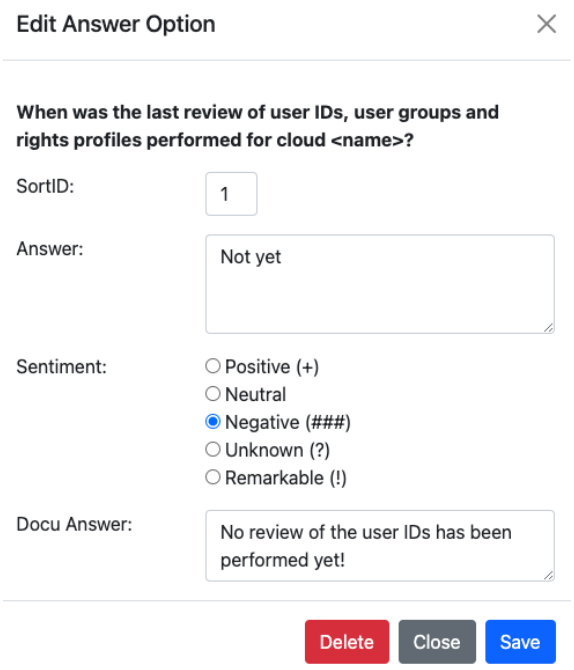


Figure 2: Sentiment specification of an answer option

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.

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

Publication details:

Status:	Published
Conference:	14th International Conference on Cloud Computing and Service Science, CLOSER 2024, Angers, France, May 2 - 4, 2024
Date of acceptance:	February 8, 2024
Full citation:	DIENER, M., BOLZ, T. (2024). Visualizing the information security maturity level of public cloud services used by public administrations. In *Proceedings of the 14th International Conference on Cloud Computing and Service Science (CLOSER)*, Angers, France (2024), pp. 543-551.
Authors' contributions:	Michael Diener 90% Prof. Dr. Thomas Bolz 10%

Conference description: The International Conference on Cloud Computing and Services Science aims at bringing together engineers, researchers and practitioners interested in advances and applications concerning the cloud infrastructure, operations, and available services through the global network. Further, the conference considers as essential the link to Services Science, acknowledging the service-orientation in most current IT-driven collaborations, and provides a forum for discussing how Services Science can provide theory, methods and techniques to design, analyze, manage, market and study various aspects of Cloud Computing.

Visualizing the information security maturity level of public cloud services used by public administrations

Michael Diener[1], Thomas Bolz[2]
[1] *University of Regensburg, Regensburg, Germany*
[2] *IU International University of Applied Sciences, Erfurt, Germany*
michael.diener@ur.de, thomas.bolz@iu.org

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

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:

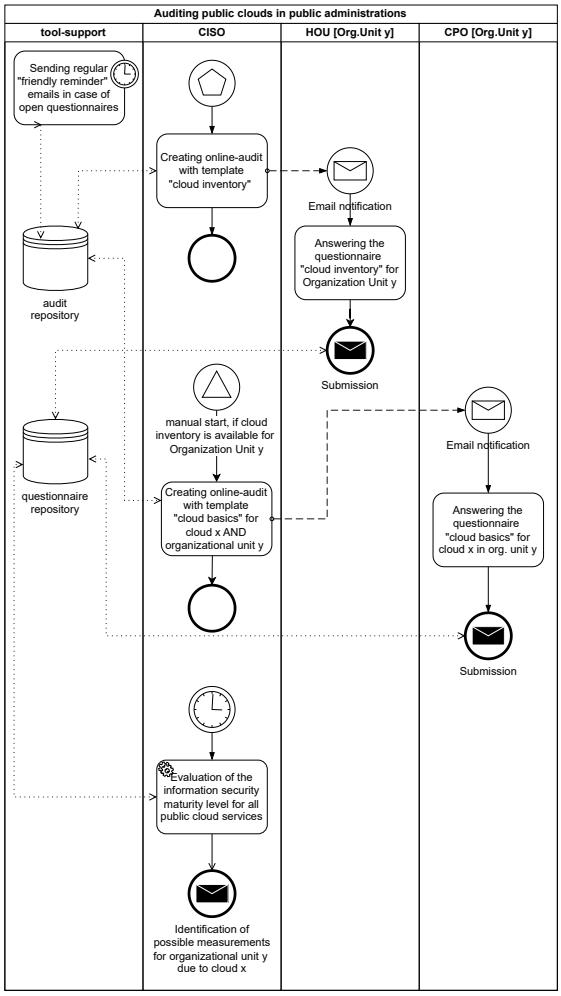


Figure 2: Holistic process of cloud security audits within public administrations

- **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.

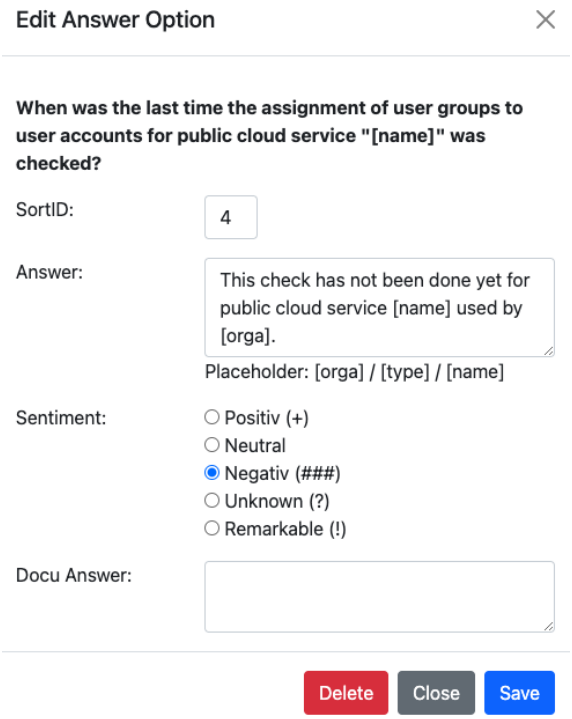


Figure 3: Predefinition of one sentiment for one of several answer-options to a single question.

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 question-

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

naires with placeholders of public cloud services for 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

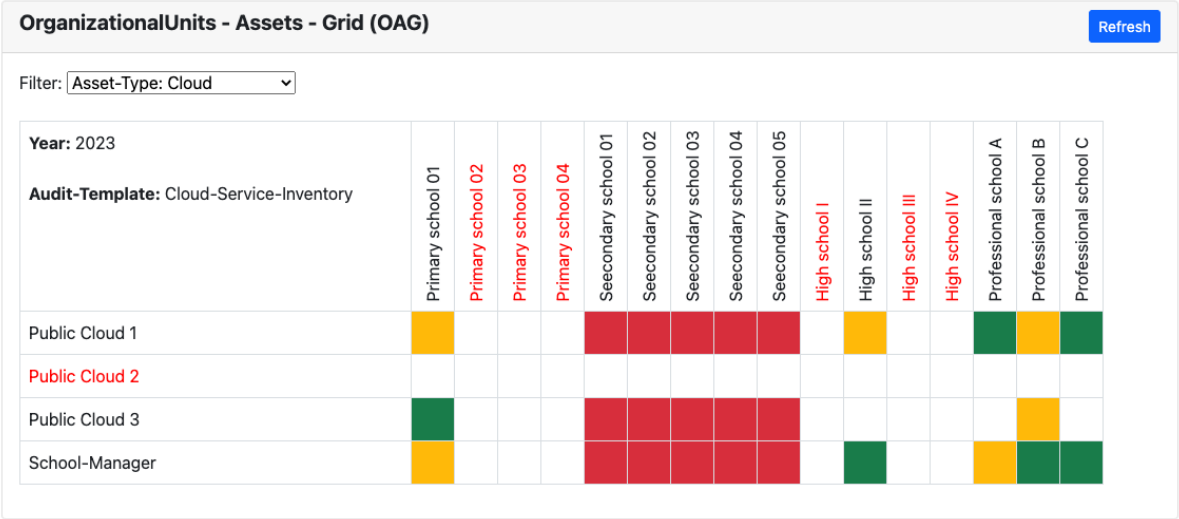


Figure 4: Visual managing support of cloud security audits within public administrations.

the schools surveyed. The OAG marks this fact with a red font color.

- 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

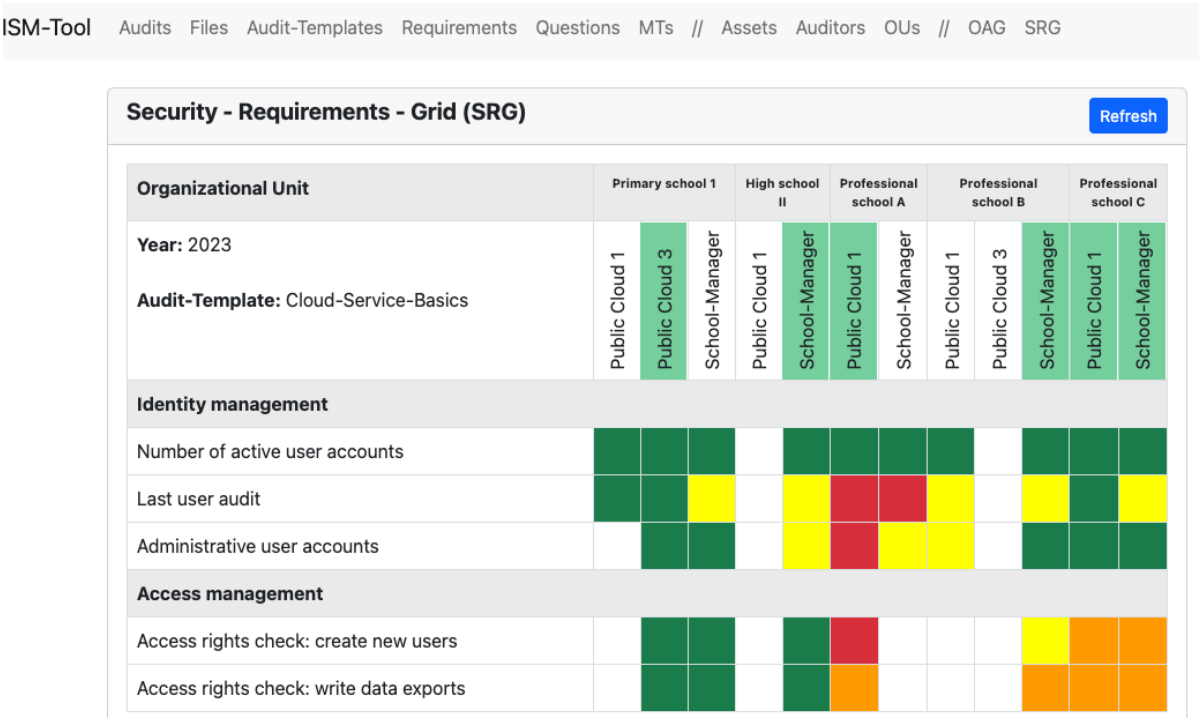


Figure 5: The SRG visualizes the information security maturity level of different public clouds.

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 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 infor-

mation 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 administra-

tions 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.

6 Utilizing cloud services in local governments as digital transformation booster by mastering information security duties

Publication details:

Status:	Under review
Journal:	Journal of Public Money & Management
Date of submission:	August 14, 2024
Full citation:	DIENER, M., MEUCHE, T. Utilizing cloud services in local governments as digital transformation booster by mastering information security duties. Submitted to: *Journal of Public Money & Management*.
Authors' contributions:	Michael Diener 90% Prof. Dr. Thomas Meuche 10%

Journal description: Public Money & Management (PMM) is a highly-respected international journal covering finance, policy and management issues in public services. PMM was started over 40 years ago by CIPFA to have an impact on global practice through high-quality research. PMM is a valuable resource for academics, politicians and policy-makers, consultants and advisors, practitioners in all types of public service organizations, journalists, and students on both academic and professional courses. PMM publishes articles which contribute new knowledge as a basis for policy or management improvements, or which reflect on evidence from public service management and finance.

Utilizing cloud services in local governments as digital transformation booster by mastering information security duties

Michael Diener[a]* and Thomas Meuche[b]

[a]*Department of Information Systems, University Regensburg, Regensburg, Germany, michael.diener@ur.de;*
[b]*Department of Business Administration, Hof University of Applied Sciences, Hof, Germany.*

Biographical notes

Michael Diener is Chief Information Security Officer at the City of Regensburg and member of the department of Business Information Systems at the University of Regensburg. In addition, he is lecturer on the "Digital Administration" degree programme at the Hof University of Applied Sciences. His research is focusing on cloud computing and information security management in public administrations and E-Government.

Thomas Meuche is Professor of Business Administration and Head of the Bachelor's degree programmes in Digital Economy and Digital Administration at Hof University of Applied Sciences. Prof. Meuche is taking the next step towards application-oriented teaching with the establishment of the "Kompetenzzentrum Digitale Verwaltung" at Hof University of Applied Sciences, whose concept he is developing together with various partners.

Disclosure statement

No potential conflict of interest was reported by the authors.

Utilizing cloud services in local governments as digital transformation booster by mastering information security duties

Impact:
The digital transformation of public administration is becoming increasingly important for Europe's competitiveness. In recent years, countless IT tools have been developed that could massively support, e.g. cloud services. Despite long-standing concerns about data protection and security in relation to public cloud services, these are now also increasingly being used in public authorities in Germany. This development has long been ignored in public administration, which means that there are now major challenges to securely managing cloud solutions. The risks of cloud information security in public administration have so far only been studied to a limited extent. The results of our study, based on the example of local authorities in Germany, show that enormous efforts must be made to use public clouds securely. This article supports policy-makers and managers with practical insights and provides an understanding of the success factors for secure cloud use in public administration.

Abstract:
Cloud services are increasingly being used to manage the digital transformation of public administrations. At the same time, the number of successful cyberattacks on the IT infrastructures has risen significantly in recent months. This empirical research analyses the status quo of public cloud services and the associated challenges and duties of information security in more than 500 local governments in Germany. Based on this, recommendations for action are derived to enhance information security of public cloud services in this domain.

Keywords:
Digital transformation, cloud computing, information security management, cybersecurity, Germany

Introduction

The digital transformation of public authorities in Europe offers enormous potential for modernising and increasing the efficiency of public services at all levels of government administration (Kuhlmann & Bogumil, 2021; Pittaway & Montazemi, 2020).

The implementation of e-government projects in the context of digital transformation must always take several levels into consideration, including data, organisational structures, processes, systems and employees (Marienfeldt et al., 2024; Otia & Bracci, 2022). According to Weerakkody et al. (2019), the increasing complexity of administrative processes means that different internal and external organisational units often have to be involved, e.g. registration of vehicles.

In the recent past, innovative platforms that support participation and collaboration between internal and external stakeholders in contrast to traditional IT systems have been implemented more and more frequently in governmental institutions (European Commission, 2023). In the scope of digital transformation, cloud services (Armbrust et al., 2010; Zaharia-Rădulescu & Radu, 2017) play a key role for government organisations, as the costs for procurement and operation are much easier to calculate (Kim et al., 2022), among other things. By using cloud services, digital platforms can be realised quickly and flexibly to design new and improved use cases (Cordella & Paletti, 2019; Johnston & Fenwick, 2024), i.e. Smart-City-Infrastructures and Urban-Data-Platforms.

Digitisation drivers in public administrations

External drivers for the implementation of such transformation projects (Kitsios et al., 2023) can be found on the one hand in legal requirements, i.e. "Single Digital Gateway" in relation to EU Regulation 2018/1724 (European Union, 2018).

On the other hand, Benbunan-Fich et al. (2020) describe, that the pressure on public administrations is growing enormously as a result of technological progress, i.e. integration of artificial intelligence (AI) applications, big data/analytics, open government data, etc. Usually, AI knowledge models require gigantic computing power, which is currently provided for the use of AI applications by powerful and flexible cloud services (i.e. Amazon Web Services, Google Compute Engine, etc.).

The Covid-19 pandemic has had a massive impact on local government in particular, both as an external and internal driver of digital transformation (Kuhlmann et al., 2021). On the one hand, new laws were passed at very short notice to deal with the crisis. New platforms and IT services had to be implemented to fulfil legal tasks, e.g. online appointment allocation. On the other hand, internal workflows had to be reorganised using innovative cloud services, e.g. home office and video conferencing, to overcome the shortage of resources.

As a massive internal driver of digital transformation, the focus is primarily on the consequences of demographic change (Colley, 2014) as many employees from the baby boomer generation are currently retiring. At the same time, it is becoming increasingly difficult to recruit qualified employees in the IT sector in local government (Maj-Waśniowska & Jedynak, 2020).

However, these drivers are pushing digitalisation forward under pressure to overcome structural and cultural barriers (Tangi et al., 2020). Automating and streamlining complex processes within public administrations will enable better use of limited resources and cost reductions. At the same time, the quality of service for citizens can be increased as digital solutions facilitate access to services and consequently increase their satisfaction.

Status quo: digital transformation vs. cybersecurity

The Digital Economy and Society Index (DESI) is published annually by the European Commission (European Commission, 2024a) and analyses various dimensions of digitalisation, including the digitalisation of public services. Above all, the Scandinavian countries are at the top of the DESI ranking. Germany is the third largest economy in the world after the United States and China, and the largest within the EU. In terms of the "digitalisation of public services" dimension, Germany is only below average according to the DESI ranking, although improvements have been made in recent years (Bánhidi et al., 2020; European Commission, 2022).

In contrast, the e-government benchmark 2024 shows that the EU member states have to make considerable investments in cybersecurity capabilities in order to protect digital supply chains and infrastructure (European Commission, 2024b). Such investments are urgently needed, as the overall number of cyberattacks is increasing dramatically. The ENISA (2023) threat landscape report provides a comprehensive overview of the status quo of cyber security in the European Union. It clearly shows that the number of incidents analysed most frequently threaten the public administration (19%). The most common types of cyberattacks are ransomware attacks (data decryption after payment of a ransom) and DDoS attacks (overloading IT systems with senseless requests leads to system crashes). Like everywhere else in the world, more and more organisations in the private and public sectors are becoming victims of cyberattacks in Germany. The Federal Office for Information Security (BSI) publishes the annual State of IT Security in Germany report (BSI, 2023). This report explains that more than 21,000 infected systems are identified and reported every day. This also includes cloud services, as these can be accessed directly via the internet.

Research scope

For these reasons, in this article we look at the utilization of external cloud services, which can significantly boost the digital transformation in public administrations. In this context, we analyse the status quo of the level of information security of cloud systems at the level of local governments in Germany. We are guided by the following research questions:

- RQ 1: How intensively are cloud services already being used in German authorities at local level?
- RQ 2: What success factors/requirements are necessary to enhance information security of cloud services in public administrations?
- RQ 3: What is the current state of information security for cloud services in public authorities in Germany?

Firstly, we explain background information and terms in the context of cloud computing and information security. We then provide an overview of related work that deals with this research topic. Next, we explain the methodological approach used to answer our research questions. Based on this, we present and discuss the results of our empirical online survey. Finally, we provide a summary of the most important findings of this work and point out limitations of this work.

Background information

Cloud computing

The term was defined by the National Institute of Standards and Technology (NIST). Cloud computing is a model in which data, programs and systems are not operated in local data centres, instead in remote IT resources (Mell & Grance, 2011). A "cloud" symbol is always used in explanations to characterise this paradigm. This makes it clear that global access to cloud data via the internet is possible for various players - as long as they are authorised.

The NIST definition describes cloud computing by differentiating between three service models, four deployment models (private, public, hybrid and community cloud) and five key characteristics of cloud resources. Armbrust et al. (2010) define the public cloud as specific IT services that can be used by anyone via the internet after payment, e.g. artificial intelligence language models, file sharing services, video conferencing solutions, etc.

The use of public cloud services offers immense advantages for public administrations, as innovative IT services do not have to be installed in their own data centre, which is costly and time-consuming. Especially in local authorities with limited financial and human resources, the digital transformation can be realised in this way. As a result of cloud utilisation, the IT infrastructure required for use cases becomes more flexible, cost-effective and scalable (Janssen & Joha, 2011). However, the security risks associated with the use of external cloud services must also be managed.

The European Commission is significantly advancing the practical applicability of cloud computing for EU citizens, the private sector and public administration with several initiatives (cf. EU Data Strategy). The aim is to enable the shared use of data in sovereign IT environments (Rone, 2024). Gaia-X is an EU-funded research project that

was launched in 2019 and is driving the development of a powerful, secure, sovereign and trustworthy data platform in compliance with European legislation. Stakeholders from research, business and administration around the world are involved in the development of this ecosystem. However, very few concepts and tools are currently available for practical use. As a result, users of public cloud services are themselves increasingly responsible for complying with legal obligations regarding data protection and information security.

Information security management

In contrast to data protection (cf. EU-GDPR), information security is not just about protecting personal data, but all processed data that is handled in organisations, processes and systems. Consideration of the "human factor" is also an essential component. The aim of information security is always to guarantee the three baseline security objectives (confidentiality, integrity and availability). The resulting security measures (e.g. concepts, guidelines, configurations, tools, etc.) must be implemented in an organisation. For this reason, regular audits are required to evaluate the effectiveness of these security measures.

In order to support the management of information security activities for Chief Information Security Officers (CISO), various standards can be applied that fall under the term Information Security Management Systems (ISMS). These define standardised processes and methods for predefined scopes of IT architectures, so that a comprehensive implementation of information security is enforced. The results can be documented by external experts by means of certifications (Disterer, 2013).

In practice, the international standard ISO/IEC 27001 is most commonly used as the ISMS standard. In Germany, the Federal Office for Information Security (BSI) has developed the "BSI IT-Grundschutz" standard (BSI, 2022), which overlaps with the

international ISO standard in many areas, although the security requirements are much more specific. Authorities and public administrations in Germany must predominantly implement the requirements of the BSI standard. In addition to these two ISMS standards, there are existing many other process models and frameworks for implementing information security.

To ensure that organisations can trust the security of public cloud services, the aforementioned ISO standard certificates are used in practice. Although these certify that the information security processes in data centres are complied with, no statement can be derived from them about how secure the "black box" of a cloud really is.

For this reason, specific cloud certifications have been developed (Banse et al., 2023; Giulio et al., 2017). Furthermore, the German BSI has developed the C5 standard, which specifies high requirements for cloud security. In practice, this is currently only offered by the major cloud service providers due to the regularly high costs of certification. The European Commission is developing the EU Cloud Certification Scheme (EUCS) for public cloud services in cooperation with the European Union Agency for Cybersecurity (ENISA), but it is not yet ready for practical application. The international framework Cloud Controls Matrix (CCM), which is being promoted by the Cloud Security Alliance, is currently also not very widespread among European cloud service providers.

In the USA, the Federal Risk and Authorisation Management Program (FedRAMP) has established an ecosystem for compliance with and regular review of standardised security requirements for cloud services (Irion, 2012). This concept is well-founded and promising, but it is not yet able to generate trust in the European member states due to the current US CLOUD Act.

In summary, it can be stated that organisations planning or already implementing cloud services for digital transformation bear full responsibility for the procurement, implementation and operation of such IT systems. In relation to our research questions, we therefore analyse the status quo of information security for cloud services in local authorities in Germany.

Related work

In general, there are many articles in the literature on the topic of information security for cloud services. There are numerous articles that deal with security frameworks, cloud migration and drivers and challenges in cloud adoption. In addition, there are many results of studies on how cloud services are used in enterprises.

In comparison, there are almost very few research contributions in the domain of public administration. We want to bridge this research gap with the results of this paper. Our search in relevant literature sources (ACM, dblp, IEEE, Google Scholar) for the search term [+"cloud service" +"information security management" +"public sector"] resulted in only a limited number of search matches that are suitable for answering our research questions. In the following, we present relevant contributions that were compiled on the basis of interviews with representatives of local authorities.

As part of an empirical research project, the adoption of cloud services and the associated cyber security challenges in public administrations in Norway were analysed (Valbø, 2023). Among other things, it was found that security processes must be fully applied to the lifecycle of cloud solutions and that comprehensive awareness training for management and IT administration is of particular relevance.

Jones et al. (2019) analysed the risks and benefits of implementing cloud technologies in government institutions using the example of local government

administrations in the United Kingdom. This research identified ten success factors that are critical to the reliable deployment of cloud services in government organisations.

Similarly, Kyriakou et al. (2020) analysed the factors that influence the decision to use cloud storage in local governments in Greece. For this purpose, a structured online survey was conducted with more than 100 Greek municipal administrations. In this context, it was determined that the perception of possible threats (e.g. unauthorised data access, data loss, etc.) as well as difficulties and efforts in the integration of cloud storage and compatibility with existing processes, business practices and the peculiarities of administrations play a crucial role.

In 2022, Choodakowska et al. (2022) published the results of their study, in which they used a representative online survey to ask 2,477 cities (70% response rate) in Poland about the status quo of information security management. In particular, they investigated the extent to which the implementation of ISMS and regular risk analyses can contribute to improving information security in local authorities. The results showed, among other things, that the respondents considered personal data and employee data to be the most vulnerable to cyberattacks, while cloud infrastructures were categorised as the least vulnerable in this respect. Not all of the hypotheses analysed were confirmed in this study.

Our literature search revealed that published scientific results for public administrations in Germany that deal with our research question are not existing. Moses et al. (2022) analysed the status quo of ISMS in local authorities in several case studies. However, the topic of cloud computing was not considered in this context.

Research methodology

To address our research questions, it is essential to conduct our own empirical study in the public administration domain due to the lack of literature sources. Therefore, we followed the suggested steps for conducting the online survey process according to Callegaro et al. (2015, p. 11) in order to obtain as much qualitative feedback as possible from several local authorities in Germany. Our applied research approach is divided into the following three stages.

Preliminary research activities (stage 1)

To develop suitable questions for our online survey, we first conducted several interviews with qualified experts from public administrations. The aim of these interviews was to develop an in-depth understanding of the research questions to be analysed. We used the digital transformation framework as a theoretical basis. Otia & Bracci (2022) designed this framework to analyse both technical and non-technical factors influencing the digital transformation of supreme audit institutions. We adopted this framework for our study and adapted it minimally for our purposes (see Figure 1).

The digital transformation framework considers five dimensions: strategy, organisation, process, people & culture and technology. These act as influencing variables on the digital transformation in local authorities as soon as technology-driven external changes occur. In our use case, the utilisation of cloud services is this external technological driver. To gain a better understanding of these dimensions, we conducted a total of five individual interviews with various experts from local governments in Germany (see Table 1).

First, we discussed potential requirements and success factors for each of the five dimensions of the digital transformation framework. In this context, we explained the significance of each influencing factor to the interviewees so that relevant aspects

from practice could be identified. Building on this, in a further step we derived essential requirements from the modules "ISMS.1 Security Management" and "OPS.2.2 Cloud Usage" of the BSI IT-Grundschutz Compendium (BSI, 2022) and assigned them to the five influencing factors (see Table 2).

Preparation of hypothesises and questionnaire (stage 2)

In the next step, we compared the findings from the interviews with the identified generalised key success factors for secure cloud utilisation in public administrations. We assigned the status quo of the local authorities surveyed to each of the five dimensions and documented them (see Table 3).

The results in table 3 show that there is almost no existing cloud strategy among the experts surveyed. There is also a lack of security guidelines for the use of cloud services in the "Process" dimension. On this basis, we have formulated the following hypotheses, which we want to test as part of this online survey:

H1: Public administrations that already have an information security policy organise voluntary or mandatory awareness training more frequently.

H2: Public administrations that do not regulate the importance of cloud services in their IT strategy are more likely to have no cloud security policies.

H3: Public administrations that already have an information security policy are more likely to document the cloud services they use.

H4: Public administrations that have IT security policies for cloud services are more likely to document the adopted cloud services.

We formulated the questions for the questionnaire in an iterative process based on the data from table 2. For quality assurance purposes, we optimised the structure of the online questionnaire several times with scientific support.

Fielding (stage 3)

In parallel, we generated a list of e-mail addresses of cities and municipalities, as central coordination of our survey with the help of a federal authority was impossible for both organisational and technical reasons.

We therefore collected public address lists on the basis of a comprehensive web search and prepared them for this purpose. As this was not possible for the majority of the federal states, we also systematically searched the internet addresses of local authorities in Germany for suitable e-mail addresses using self-developed web crawlers. The collected contact data was subsequently subjected to comprehensive quality assurance.

An identification number was also assigned to each public administration so that it could be ensured that the authorities contacted only took part in the online survey once. This also enabled us to send organisation-specific reminder emails to improve the participation rate.

After we had advertised our study in the Internet forum of the IT security officers for federal states and municipalities, an intensive e-mail marketing process took place with a time delay and in several stages. In summary, the data was collected between 1 August 2023 and 30 November 2023. After a first quality assurance, a total of 515 public administrations from Germany took part in our online survey.

Results

Implementation of Cloud Services in local governments

As part of our evaluation, we only considered authorities (n = 507) that can be assigned to the local government level. Of these, one district government, 63 counties or districts, 39 independent cities and 404 public administrations of cities, municipalities, markets or administrative communities took part. Table 4 provides an overview of the number of participating local governments (more than 200 inhabitants according to (Statistisches Bundesamt, 2022)) and their utilisation intensity of cloud services, grouped by federal state.

In order to carry out cross-evaluations, we divided the municipal administrations into three classes depending on their number of employees: small (1 - 50 employees), medium (51 - 500 employees) and large (more than 500 employees). The number of small administrations (128) comprises approx. 25.3%, the number of medium-sized administrations (255) to approx. 50.4% and the number of large institutions (124) to approx. 24.4% of the participating local authorities. By applying this categorisation, we achieve a Gaussian distribution.

One of the most important questions examined the intensity of the **adoption of public cloud services**. To ensure a standardised understanding, we provided a simplified explanation of the term immediately before the question, considering specific practical examples. The result for this question was clear. 390 of the 507 local authorities (77%) stated that they use at least one public cloud service (see Table 4).

In the **number of cloud services used**, almost 47% of respondents stated that they have implemented between one and three public cloud services. Around 35% of the local authorities surveyed use four to ten. Only 6% use more than ten cloud services.

12% of respondents were unable to quantify the number of public cloud services used in their authority.

Regarding the intended **purposes of external cloud services**, we were able to derive the following findings from the standardised text responses. According to this, public cloud services are mainly used for file sharing (approx. 32%), the operation of government information systems (approx. 22%) and the provision of portals (approx. 13%) to collaborate with citizens and businesses.

Information security in local authorities

In accordance with BSI IT-Grundschutz (see ISMS.1.A4 in (BSI, 2022)), the **role of the chief information security officer (CISO)** is of particular importance in order to ensure the implementation of security measures for compliance with the baseline security objectives (confidentiality, availability and integrity). Around 43% of the local authorities surveyed have internal CISOs for the coordination of information security. External service providers are mainly active for medium-sized (approx. 13%) and small (approx. 9%) public administrations. However, it is striking that 87 of the 507 local authorities surveyed (approx. 17%) do not currently have a defined organisational responsibility for coordinating information security.

The extent to which an **information security guideline** (see ISMS.1.A3 in (BSI, 2022)) exists was also analysed. More than 45% of the authorities surveyed have such a guideline in place. More than a quarter of respondents are currently planning to implement an information security guideline. It is remarkable that 110 public administrations (approx. 22%) do not currently have such a guideline.

In order to successfully implement the baseline security objectives, employees must be sensitised to information security (see ORP.3.A6 in (BSI, 2022)). **Mandatory information security training** has already been carried out at 222 local authorities

(approx. 44%). 85 respondents stated that awareness training had been carried out in their institution on a voluntary basis (approx. 17%). In 86 of the local authorities surveyed, information security awareness trainings are currently being planned. In 93 of the municipal administrations surveyed (approx. 18.5%), no awareness training has been carried out or planned to date (see Figure 2).

To ensure a structured implementation of security requirements, the **implementation of an information security management system (ISMS)** is essential (see ISMS.1 in (BSI, 2022)). A fifth of the 505 respondents have already implemented an ISMS in their institution. 186 of the respondents (approx. 37%) stated that an ISMS is currently being planned or set up. In contrast, 174 of the respondents (approx. 34.5 %) do not currently have an ISMS in place and are not planning to set one up.

Management of cloud services in local governments

Only 30 out of 343 (approx. 9%) currently have an **IT strategy** that describes the relevance of public cloud services (see OPS.2.2.A1 in (BSI, 2022)). 18% of respondents stated that they do have an IT strategy, but that it does not define the use of public cloud services. Around 23% of the local authorities surveyed are currently developing such a document. Almost 50% of respondents answered that an IT strategy in their authority is not existing and also not in the planning stage.

Regulations are required for the compliant operation of cloud applications, e.g. **IT security policies or service instructions**. This is to define security-related requirements for all phases of the lifecycles of cloud applications (see OPS.2.2.A2 in (BSI, 2022)). At the time of the survey, only 13% of local authorities using public cloud services had such regulations. Almost as many are currently revising their existing regulations. More than 66% of respondents do not currently have such IT security policies or instructions and are not planning to implement them.

In manage information security, the implemented cloud services must be documented (see OPS.2.2.A3 in (BSI, 2022)). Currently, only 7% of the local authorities surveyed have up-to-date **documentation of their cloud services**, although this does not show which public cloud services are used by which organisational units (see Figure 3). Nearly 20% stated that they have complete documentation of their public cloud services. Almost as many are currently in the process of updating their documentation. Just under 50% of the 342 respondents answered that they do not have a documented overview of the public cloud services used.

Overall, only around a third of the 299 local authorities surveyed have **regulations that cover the duties and responsibilities for planning, implementing and operating public cloud services** (see Figure 4). Only 17% have regulations that relate to regular reviews of technical security configurations of adopted cloud services.

In light of the fact that Microsoft's extended technical support for the Office 2016 and Office 2019 products will expire in October 2025, we asked the interviewees how they expect the **implementation of cloud-based Microsoft software solutions (e.g. Microsoft 365) in the future**. So far, only 35 of the 287 respondents (12%) have set up an internal working group to look into the future use of cloud-based Microsoft products. Almost 25% of local authorities are awaiting decisions from the relevant data protection authorities regarding the GDPR compliant operation of Microsoft 365 etc. A third stated that they had not yet considered the use of cloud-based Microsoft software solutions. The majority of respondents (approx. 60%) are in favour of operating classic Microsoft products on-premises on their own systems as long as this is technically possible.

Dependent influencing variables on the identified key success factors

To test our hypotheses, the data set was prepared for the application of the chi-square test. This test form is used to investigate nominally scaled measurement variables to determine the existence of correlations between two factors.

If a correlation exists, a binary logistic regression analysis (Harrell, 2015) was performed in addition to this to be able to make statements about the correlations between an independent variable (predictor) and the analysed dependent variable (criterion). A significance level of 5 % was set for all tests. Furthermore, we take care to ensure that applicable requirements for conducting the test were met.

- **Hypothesis 1**: The relationship between the existence of information security guidelines and the organisation of awareness training was examined. A statistically significant correlation was found in this regard, $\tilde{\chi}^2(1) = 77.41$, $p = <0.001$, Cramér's $V = 0.4$.

  The logistic regression analysis was performed to determine the influence of existing information security guidelines on the dependent variable (awareness training has taken place). The calculated model as a whole is significant ($\tilde{\chi}^2(1) = 77.74$, $p <0.001$, $n = 378$). The coefficient for the dependent variable (information security guideline exists) is $b = 2.03$ and is therefore positive. The odds ratio is 7.6 and illustrates the increased dependency between the two variables.

- **Hypothesis 2**: There is a statistically significant relationship between the existence of IT strategies and the existence of IT security policies for cloud services, $\tilde{\chi}^2(1) = 107.71$, $p = <0.001$, Cramér's $V = 0.68$.

  The logistic regression analysis showed that the model as a whole is significant ($\tilde{\chi}^2(1) = 77.74$, $p <0.001$, $n = 236$). The coefficient for the

independent variable (IT strategy regulates the use of public cloud services) is b = 4.31 and is positive. The odds ratio = 74.37 and illustrates the massive influence between the existence of an IT strategy and the existence of IT security policies for public cloud services.

- **Hypothesis 3**: A correlation between the existence of information security guidelines and the documentation of public cloud services could not be established as there is no statistical significance, $\tilde{\chi}^2(2) = 3.68$, $p = 0.159$, Cramér's V = 0.12. As the specified significance level is exceeded, there is no significant correlation between the two influencing variables analysed. Therefore, Hypothesis 3 cannot be confirmed.
- **Hypothesis 4**: The influence of IT security policies for public cloud services on the documentation of the cloud applications used was analysed. A statistically significant correlation was found in this regard, $\tilde{\chi}^2(2) = 34.2$, $p = <0.001$, Cramér's V = 0.38.

  A logistic regression analysis was performed to determine the influence of the existence of IT security policies for public cloud services on the dependent variable (documentation of cloud services). This showed that the calculated model as a whole is significant ($\tilde{\chi}^2(1) = 30.68$, $p <0.001$, $n = 208$). The coefficient b = 2.25 is positive and describes that if the existence of such an IT security policy is positive, the probability increases that the dependent variable (cloud documentation exists) also behaves positively. The calculated odds ratio is 9.53 for this analysed correlation.

Discussion

Practical implications

The results of our research show due to RQ 1 that public cloud services have now become an integral part of the IT landscapes of local governments in Germany. In detail, this means that 70.3% of small, 76.9% of medium-sized and 83.9% of large public administrations use external cloud services. It can therefore be concluded that the larger an administration is, the more likely it is to use public cloud services.

Regarding RQ 2, we have identified seven important key success factors (see Table 2) in relation to the digital transformation framework enhancing the information security of cloud services in public authorities. The basic prerequisite is an IT strategy and a CISO who establishes an ISMS. In addition, the existence of an information security guideline and specific cloud security guidelines is important. The mandatory implementation of cloud documentation must be regulated in the cloud security guidelines. Regular security awareness training for employees is important to ensure that the human factor is taken into account in the cloud security processes.

In relation to RQ 3, we have identified that there are a lot of shortcomings in cloud information security processes in German authorities: 12% of respondents were unable to quantify the number of public cloud services adopted in their authority. This could possibly be due to a lack of documentation (see Figure 3). Accordingly, the probability that implemented public cloud services are inadequately secured with technical and organisational security measures is likely to increase significantly under such conditions. In practical terms, this means that more IT security incidents related to adopted cloud services can be expected in the future.

Currently, 21.7% of the public administrations surveyed do not have an information security guideline. This means that these authorities also lack a clear

commitment from the administrative management to assume overall responsibility for information security. Consequently, there is a lack of a central message to the employees that IT security plays an essential role in daily administrative operations. This increases the likelihood that detailed IT security regulations for the secure operation of public cloud services will be lacking in such organisations. There is also a risk of unregulated responsibilities with regard to the functional and technical administration of outsourced IT services.

More than 18% of the participating local authorities have not yet conducted or planned any awareness training campaign for information security. Due to the recent sharp rise in the number of IT security incidents in local governments, it is time to implement such security measures without delay. There are already many e-learning providers on the market that offer high-quality training courses.

Almost 50% of respondents answered that they do not have an IT strategy in their organisation. However, without strategic guidelines from management board, it is difficult to utilise future IT technologies in public administrations in a targeted and secure manner. In combination with the information security guideline, the foundation for specific guidelines and regulations would be given to define planning, integration and operation of public cloud services.

Theoretical implications

The results of our study also have a direct influence on scientific findings. In addition to information security guidelines and security awareness training, there is currently a massive lack of ISMS implementations in public administrations. Against this background, further empirical studies should be carried out to determine possible reasons and hurdles in this domain.

In addition, the applicability of existing maturity models for determining the status quo of information security of cloud services in public administrations should be analysed in more detail. There are currently only a few articles in the literature that deal with this issue in this area of application.

With regard to network theory, it is necessary to critically examine how ubiquitous IT services can be provided centrally for local governments by superordinate authorities, taking into account the principles of federalism. In accordance with the "one-for-all"-principle, secure and customisable web solutions could be published that can be adopted by all authorities in Europe, analogous to the US FedRAMP concept.

Conclusions

This study analysed the status quo of the use of cloud services in public administrations in Germany based on a representative empirical online survey. The questionnaire was developed with the support of expert interviews based on the theory of digital transformation frameworks. The survey focussed on IT managers and information security officers at local governments. We identified key elements of information security management that are essential for the secure operation of external cloud resources. Overall, the following key findings were identified:

1. Currently, 17% of the local authorities surveyed have unregulated responsibility for coordinating information security. This is predominantly the case for authorities with between 51 and 500 employees. One fifth of respondents currently lack an information security guideline. More than 18% have not yet carried out any information security awareness training. Currently, only around 20% of the public administrations surveyed have implemented an ISMS.

2. Almost 80% of the institutions surveyed use public cloud services. More than 40% of local governments that use public cloud services do not have an IT strategy that regulates their overall utilisation. However, there is a strong correlation between the existence of an IT strategy and specific cloud security policies.
3. Around 50% of local authorities that use public cloud services do not have a documented overview of these assets. As a result, it is highly likely that there is a lack of suitable technical and organisational security measures, which opens the door to cyberattacks.

Nevertheless, there were some limitations in the context of this research work. For example, due to federalism in Germany, it was not possible to conduct an even more meaningful online survey. Overall, this study focussed only on local governments, meaning that state and federal authorities in Germany could not be considered.

In this respect, future research in this domain should be expanded accordingly to determine a complete picture of the status quo of public cloud services in German authorities. Furthermore, this online survey should be repeated and conducted in other European countries so that a meaningful comparison would be possible.

Ultimately, due to the shortage of IT specialists and the increasing provision of cloud-based software solutions, the implementation of cloud services in public authorities has become indispensable. Despite this, our results show that enormous efforts will be required to ensure that the digitisation of public administration is a success. It is to be hoped that concepts such as Gaia-X Cloud, Delos Cloud, dPhoenix-Suite etc. will help to structurally and securely advance the digital transformation of public administrations.

References

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50–58. https://doi.org/10.1145/1721654.1721672

Bánhidi, Z., Dobos, I., & Nemeslaki, A. (2020). What the overall Digital Economy and Society Index reveals: A statistical analysis of the DESI EU28 dimensions. *Regional Statistics*, *10*(2), 42–62. https://doi.org/10.15196/rs100209

Banse, C., Kunz, I., Haas, N., & Schneider, A. (2023). A Semantic Evidence-based Approach to Continuous Cloud Service Certification. *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, 24–33. https://doi.org/10.1145/3555776.3577600

Benbunan-Fich, R., Desouza, K. C., & Andersen, K. N. (2020). IT-enabled innovation in the public sector: introduction to the special issue. *European Journal of Information Systems*, *29*(4), 323–328. https://doi.org/10.1080/0960085X.2020.1814989

BSI. (2022). *BSI IT-Grundschutz-Compendium Edition 2022*. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.html

BSI. (2023). *The State of Security in Germany 2023*. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2023.html

Callegaro, M., Manfreda, K. L., & Vehovar, V. (2015). *Web Survey Methodology*. SAGE Publications Ltd. https://doi.org/10.4135/9781529799651

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

Journal of Local Self-Government, *20*(1), 161–192. https://doi.org/10.4335/20.1.161-192(2022)

Colley, L. (2014). Understanding Ageing Public Sector Workforces: Demographic challenge or a consequence of public employment policy design? *Public Management Review*, *16*(7), 1030–1052. https://doi.org/10.1080/14719037.2013.771697

Cordella, A., & Paletti, A. (2019). Government as a platform, orchestration, and public value creation: The Italian case. *Government Information Quarterly*, *36*(4), 101409. https://doi.org/10.1016/J.GIQ.2019.101409

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*(02), 92–100. https://doi.org/10.4236/jis.2013.42011

ENISA. (2023). *ENISA threat landscape 2023: July 2022 to June 2023*. https://doi.org/10.2824/782573

European Commission. (2022). *Digital Economy and Society Index (DESI) 2022*. https://ec.europa.eu/newsroom/dae/redirection/document/88764

European Commission. (2024a). *DESI dashboard for the Digital Decade (2023 onwards)*. https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi/charts/desi-indicators

European Commission. (2024b). *eGovernment Benchmark 2024 insight report: Advancing Pillars in Digital Public Service Delivery*. https://ec.europa.eu/newsroom/dae/redirection/document/106742

European Commission, Joint Research Centre, & Errandonea, L. (2023). *Exploring the impact of digital transformation on public governance – A community perspective*. Publications Office of the European Union. https://doi.org/doi/10.2760/679503

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 (Text with EEA relevance.)*. https://doi.org/https://eur-lex.europa.eu/eli/reg/2018/1724/oj

Giulio, C. Di, Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R. H., & Bashir, M. N. (2017). Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security? *Proceedings of the 10th IEEE International Conference on Cloud Computing (CLOUD)*, 50–57. https://doi.org/10.1109/CLOUD.2017.16

Harrell, F. E. (2015). Binary Logistic Regression. In *Regression Modeling Strategies: With Applications to Linear Models, Logistic and Ordinal Regression, and Survival Analysis* (pp. 219–274). Springer International Publishing. https://doi.org/10.1007/978-3-319-19425-7_10

Irion, K. (2012). Government Cloud Computing and National Data Sovereignty. *Policy & Internet*, *4*(3–4), 40–71. https://doi.org/https://doi.org/10.1002/poi3.10

Janssen, M., & Joha, A. (2011). CHALLENGES FOR ADOPTING CLOUD-BASED SOFTWARE AS A SERVICE (SAAS) IN THE PUBLIC SECTOR. In null s.n. (Ed.), *Proceedings of the European Conference on Information Systems (ECIS)* (pp. 1–10). Association of the Information Systems (AIS). https://aisel.aisnet.org/ecis2011/80

Johnston, L., & Fenwick, J. (2024). New development: Public service innovation. *Public Money & Management*, 1–6. https://doi.org/10.1080/09540962.2024.2362873

Jones, S., Irani, Z., & Sivarajah, U. (2019). Risks and Rewards of Cloud Computing in the UK Public Sector: a Reflection on Three Organisational Case Studies. *Information Systems Frontiers*, *21*. https://doi.org/10.1007/s10796-017-9756-0

Kim, S., Andersen, K. N., & Lee, J. (2022). Platform Government in the Era of Smart Technology. *Public Administration Review*, *82*(2), 362–368. https://doi.org/https://doi.org/10.1111/puar.13422

Kitsios, F., Kamariotou, M., & Mavromatis, A. (2023). Drivers and Outcomes of Digital Transformation: The Case of Public Sector Services. *Information*, *14*(1), 43. https://doi.org/10.3390/info14010043

Kuhlmann, S., & Bogumil, J. (2021). The Digitalisation of Local Public Services. Evidence from the German Case. In T. Bergström, J. Franzke, S. Kuhlmann, & E. Wayenberg (Eds.), *The Future of Local Self-Government: European Trends in Autonomy, Innovations and Central-Local Relations* (pp. 101–113). Springer International Publishing. https://doi.org/10.1007/978-3-030-56059-1_8

Kuhlmann, S., Bouckaert, G., Galli, D., Reiter, R., & Hecke, S. Van. (2021). Opportunity management of the COVID-19 pandemic: testing the crisis from a global perspective. *International Review of Administrative Sciences*, *87*(3), 497–517. https://doi.org/10.1177/0020852321992102

Kyriakou, N., Euripides, L., & Paraskevi, D. (2020). Factors affecting cloud storage adoption by Greek municipalities. *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance*, 244–253. https://doi.org/10.1145/3428502.3428537

Maj-Waśniowska, K., & Jedynak, T. (2020). The Issues and Challenges of Local Government Units in the Era of Population Ageing. *Administrative Sciences*, *10*(2), 36. https://doi.org/10.3390/admsci10020036

Marienfeldt, J., Wehmeier, L. M., & Kuhlmann, S. (2024). Top-down or bottom-up digital transformation? A comparison of institutional changes and outcomes. *Public Money & Management*, 1–10. https://doi.org/10.1080/09540962.2024.2365351

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. *National Institue of Standards and Technology*, *800*(145), 1–7.

Moses, F., Sandkuhl, K., & Kemmerich, T. (2022). Information security management in German local government. *Communication Papers of the 17th Conference on Computer Science and Intelligence Systems, FedCSIS 2022*, *32*(32), 183–189. https://doi.org/10.15439/2022F162

Otia, J. E., & Bracci, E. (2022). Digital transformation and the public sector auditing: The SAI's perspective. *Financial Accountability & Management*, *38*(2), 252–280. https://doi.org/10.1111/faam.12317

Pittaway, J. J., & Montazemi, A. R. (2020). Know-how to lead digital transformation: The case of local governments. *Government Information Quarterly*, *37*(4), 101474. https://doi.org/10.1016/J.GIQ.2020.101474

Rone, J. (2024). 'The sovereign cloud' in Europe: diverging nation state preferences and disputed institutional competences in the context of limited technological capabilities. *Journal of European Public Policy*, *31*(8), 2343–2369. https://doi.org/10.1080/13501763.2024.2348618

Statistisches Bundesamt. (2022). *Gemeinden nach Bundesländern und Einwohnergrößenklassen am 31.12.2022*. https://www.destatis.de/DE/Themen/Laender-R egionen/Regionales/_inhalt.html

Tangi, L., Janssen, M., Benedetti, M., & Noci, G. (2020). Barriers and Drivers of Digital Transformation in Public Organizations: Results from a Survey in the Netherlands. In G. Viale Pereira, M. Janssen, H. Lee, I. Lindgren, M. P. Rodríguez Bolívar, H. J. Scholl, & A. Zuiderwijk (Eds.), *Electronic Government* (pp. 42–56). Springer International Publishing.

Valbø, T. (2023). *Cloud adoption and cyber security in public organizations: an empirical investigation on Norwegian municipalities* [University of Agder]. https://hdl.handle.net/11250/3078638

Weerakkody, V., El-Haddadeh, R., Sivarajah, U., Omar, A., & Molnar, A. (2019). A case analysis of E-government service delivery through a service chain dimension. *International Journal of Information Management*, *47*, 233–238. https://doi.org/10.1016/J.IJINFOMGT.2018.11.001

Zaharia-Rădulescu, A.-M., & Radu, I. (2017). Cloud computing and public administration: approaches in several European countries. *Proceedings of the International Conference on Business Excellence*, *11*(1), 739–749. https://doi.org/doi:10.1515/picbe-2017-0078

Figure 1: Digital transformation framework (based on Otia and Bracci, 2022)

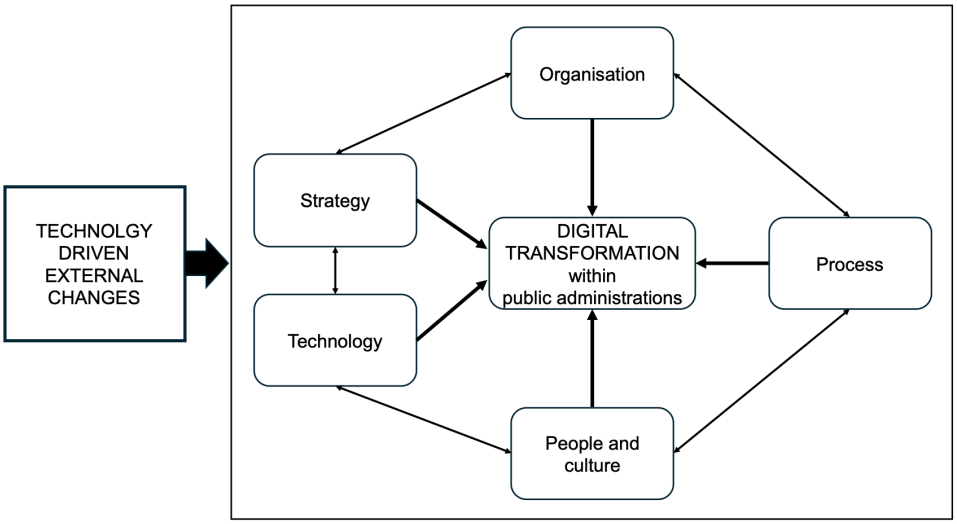


Table 1: Summary of interviewees

No.	Job position	Type of authority	Duration of interview	Region	Medium
1	Data protection officer	City administration	49 min	South Bavaria	Personal
2	CISO	City administration	33 min	North Bavaria	Telephone
3	IT Manager	Municipal administration	58 min	North Bavaria	Personal
4	CISO	City administration	41 min	South Bavaria	Telephone
5	External IT consultant	Local authority	36 min	North Bavaria	Personal

Table 2: Key success factors for utilizing cloud services in public administrations related to security requirements of BSI IT-Grundschutz Compendium

Dimension of digital transformation framework	Generalized key success factors for secure cloud utilization in public administrations	Requirements of BSI IT-Grundschutz Compendium
Strategy	A strategy for public cloud services is required (goals, opportunities and risks that the public administration associates with cloud adoption).	OPS.2.2.A1
Organization	Establishing an information security guideline that describes the importance of information security, the objectives, the most important aspects of the security strategy and the organisational structure for information security.	ISMS.1.A3
	A chief information security officer (CISO) needs to be appointed to manage the essential security processes within the organisation.	ISMS.1.A4
Process	A security policy for cloud use must be developed based on the cloud strategy (contains specific security requirements for integration of public cloud services, i.e. identity and access management).	OPS.2.2.A2
	Information security for cloud services needs to be implemented in all related business processes to ensure that all necessary security aspects are taken into account not only for new processes and projects, but also for ongoing activities.	ISMS.1.A9
Technology	A service definition needs to be developed for each adopted cloud service.	OPS.2.2.A3
	An Up-to-date documentation of the used cloud assets is mandatory; regular security audits of public cloud services based on cloud security policy.	OPS.2.2.A4
People and culture	Mandatory awareness trainings are mandatory to address cyber risks in context of cloud usage.	ISMS.1.A8

Table 3: Status quo - implementation of security requirements for cloud services

No.	Type of authority	Use of Cloud Services	Strategy	Organisation	Process	Technology	People and culture
1	City administration	yes	no	yes	no	partly	yes
2	City administration	yes	partly	yes	yes	partly	yes
3	Municipal administration	yes	no	no	no	no	no
4	City administration	yes	no	yes	no	no	partly
5	Local authority	yes	no	no	no	no	no

Table 4: Participating local governments and intensity of adoption of cloud services

Federal state	Cities > 200 inhabitants	Participating municipalities	Participating municipalities (rel.)	Adoption of cloud services	Adoption of cloud services (rel.)
Baden-Württemberg	1.095	75	6,8 %	61	81,3 %
Bayern	2.056	111	5,4 %	88	79,3 %
Berlin	1	1	100,00 %	0	0,0 %
Brandenburg	413	21	5,1 %	16	76,2 %
Bremen	2	0	0 %	0	0,0 %
Hamburg	1	1	100,0 %	1	100,0 %
Hessen	422	54	12,8 %	38	70,4 %
Mecklenburg-Vorpommern	692	10	1,4 %	7	70,0 %
Niedersachsen	941	44	4,7 %	36	81,8 %
Nordrhein-Westfalen	396	69	17,4 %	52	75,4 %
Rheinland-Pfalz	1.914	31	1,6 %	20	64,5 %
Saarland	52	8	15,4 %	7	87,5 %
Sachsen	419	38	9,1 %	29	76,3 %
Sachsen-Anhalt	218	13	6,0 %	10	76,9 $ %
Schleswig-Holstein	967	9	0,9 %	7	77,8 %
Thüringen	546	22	4,0 %	18	81,9 %
	10.135	507	5,0 %	390	77,0 %

Figure 2: Implementation of awareness training for information security in public administrations

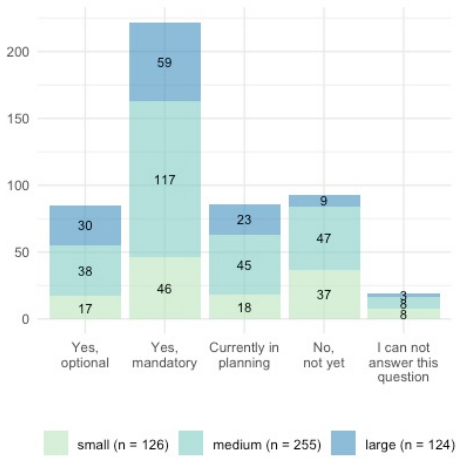


Figure 3. Documentation of public cloud services in local governments

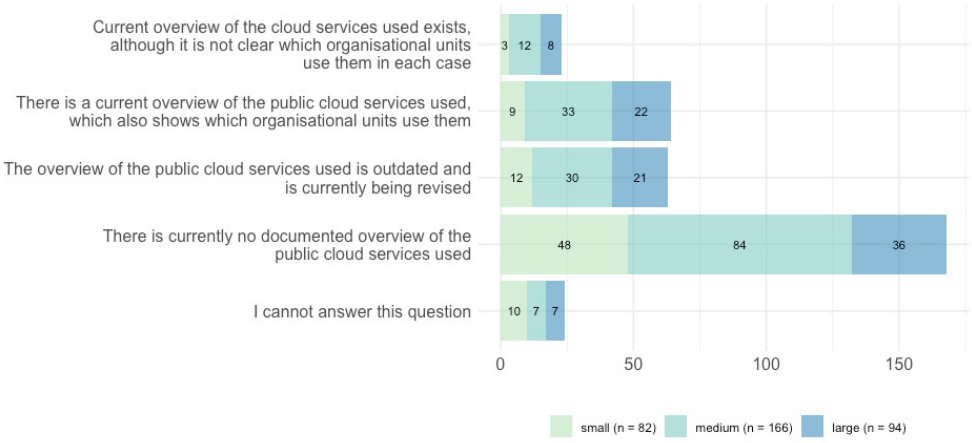
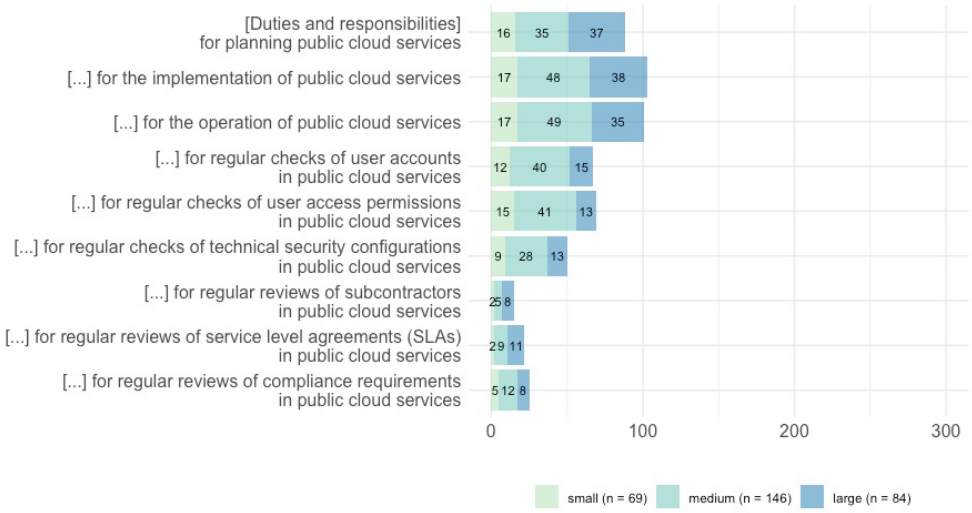


Figure 4. Regulations for managing the information security of public cloud services in municipal administrations (multiple answers possible)



Bibliography

[1] ALVARENGA, A., MATOS, F., GODINA, R., AND MATIAS, J. C. O. Digital transformation and knowledge management in the public sector. *Sustainability 12* (2020).

[2] ANDRONICEANU, A. The new trends of digital transformation and artificial intelligence in public administration. *Administratie si Management Public 40* (2023), 147–155.

[3] ARMBRUST, M., FOX, A., GRIFFITH, R., JOSEPH, A. D., KATZ, R., KONWINSKI, A., LEE, G., PATTERSON, D., RABKIN, A., STOICA, I., AND ZAHARIA, M. A view of cloud computing. *Communications of the ACM 53* (9 2010), 50–58.

[4] ASSAF, A., IISHAMSIR, A. W., AND MUHAMMAD, M. Benefits and risks of cloud computing in e-government tasks: A systematic review. *E3S Web of Conferences 328* (12 2021).

[5] BLANCATO, F. G. The cloud sovereignty nexus: How the european union seeks to reverse strategic dependencies in its digital ecosystem. *Policy & Internet 16* (2024), 12–32.

[6] BOBAN, M., AND KLARIĆ, M. Impact of covid 19 pandemic on digital transformation of public administration in european union. In *2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO)* (2021), pp. 1312–1317.

[7] BRANCO, I. C. J. T., AND FONSECA. Verifying the situation of cybersecurity in portugal's municipalities. In *Information Systems and Technologies* (2024), Hojjat, D. Gintautas, M. Fernando, C. V. R. Alvaro, and Adeli, Eds., Springer Nature Switzerland, pp. 176–186.

[8] BRAUD, A., FROMENTOUX, G., RADIER, B., AND GRAND, O. L. The road to European digital sovereignty with Gaia-X and IDSA. *IEEE Network 35* (9 2021).

[9] BRZOZOWSKA-RUP, K., NOWAKOWSKA, M., AND ZDRADZISZ, M. Cloud computing in the polish public administration: current state and development prospects. *Technological Forecasting and Social Change 205* (2024), 123500.

[10] BSI. Cloud Computing Compliance Criteria Catalogue, 2020.

[11] BSI. BSI IT-Grundschutz-Compendium Edition 2022, 2022.

[12] BSI. The State of Security in Germany 2023, 2023.

[13] BURGFRIED, M., AND RECKERT-LODDE, A. Die Deutsche Verwaltungscloud-Strategie. *Datenschutz und Datensicherheit - DuD 46* (2022), 611–615.

[14] CALLEGARO, M., MANFREDA, K., AND VEHOVAR, V. *Web Survey Methodology*. Sage, 1 2015.

[15] CHOODAKOWSKA, A., KAŃDUŁA, S., AND PRZYBYLSKA, J. Cybersecurity in the local government sector in poland: More work needs to be done. *Lex localis - Journal of Local Self-Government 20* (2022), 161–192.

[16] CLOHESSY, T., ACTON, T., AND MORGAN, L. Smart city as a service (scaas): A future roadmap for e-government smart city cloud computing initiatives. In *2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing* (2014), pp. 836–841.

[17] COURSEY, D., AND NORRIS, D. F. Models of e-government: Are they correct? an empirical assessment. *Public Administration Review 68* (2008), 523–536.

[18] CSA. Cloud Control Matrix, 2021.

[19] DAVID, A., YIGITCANLAR, T., LI, R. Y. M., RODRÍGUEZ, J. C., CHEONG, P., MOSSBERGER, K., AND MEHMOOD, R. Understanding local government digital technology adoption strategies: A prisma review. *Sustainability 15* (8 2023), 9645.

[20] DOUBRAVA, C., AND SIKES, V. Cloud-Paradigma in der öffentlichen Verwaltung. *Datenschutz und Datensicherheit - DuD 2022 46:10 46* (9 2022), 605–610.

[21] EL-GAZZAR, R., AND WAHID, F. Strategies for cloud computing adoption: Insights from the norwegian public sector, 8 2015.

[22] ENISA. EUCS – Cloud Services Scheme. 1–245.

[23] ENISA. ENISA threat landscape 2023: July 2022 to June 2023, 2023.

[24] HEVNER, A. R., MARCH, S. T., PARK, J., AND RAM, S. Design science in information systems research. *MIS Quarterly 28* (2004), 75–105.

[25] HOLDEN, S. H., NORRIS, D. F., AND FLETCHER, P. D. Electronic government at the local level: Progress to date and future issues. *Public Performance & Management Review 26* (2003), 325–344.

[26] ISLAM, M. S., AND KARLSSON, F. The public sector cloud service procurement in sweden: An exploratory study of use and information security challenges. *International Journal of Public Administration in the Digital Age (IJPADA) 8* (2021), 1–22.

[27] ISMAGILOVA, E., HUGHES, L., RANA, N. P., AND DWIVEDI, Y. K. Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework. *Information Systems Frontiers 24* (2022), 393–414.

[28] ISO CENTRAL SECRETARY. Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, 2019.

[29] J., H. L., RENÉ, R., AND ARMIN, H. *Forschungsmethoden der Wirtschaftsinformatik*. Springer Berlin Heidelberg, 2011, pp. 97–109.

[30] JANJA, M. N., AND VINTAR. Technology as the key driver of organizational transformation in the egovernment period: Towards a new formal framework. In *Electronic Government* (2011), H. J., W. M. A., T. Y. hua Janssen Marijn, and Scholl, Eds., Springer Berlin Heidelberg, pp. 453–464.

[31] JANSSEN, M., AND JOHA, A. Challenges for adopting cloud-based software as a service (saas) in the public sector. In *Proceedings of the 19th European Conference on Information Systems (ECIS)* (8 2011).

[32] JONES, S., IRANI, Z., AND SIVARAJAH, U. Risks and rewards of cloud computing in the uk public sector: a reflection on three organisational case studies. *Information Systems Frontiers 21* (4 2019).

[33] JOOS, H. Hochskalierbares Cloud Computing mit nationalen Hyperscalern für die Verwaltung. *Datenschutz und Datensicherheit - DuD 46* (2022), 699–702.

[34] KARYDA, M., BALOPOULOS, T., DRITSAS, S., GYMNOPOULOS, L., KOKOLAKIS, S., LAMBRINOUDAKIS, C., AND GRITZALIS, S. An ontology for secure e-government applications. In *First International Conference on Availability, Reliability and Security (ARES'06)* (4 2006), pp. 5 pp.–1037.

[35] KPMG. Cloud Monitor 2021: Es wird voll in der Wolke, 2021.

[36] KPMG. Cloud Monitor 2023, 2023.

[37] KUIPER, E., DAM, F. V., REITER, A., AND JANSSEN, M. Factors influencing the adoption of and business case for cloud computing in the public sector, 2014.

[38] KYRIAKOU, N., EURIPIDES, L., AND PARASKEVI, D. Factors affecting cloud storage adoption by greek municipalities. In *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance* (2020), Association for Computing Machinery, pp. 244–253.

[39] LABES, S., HAHN, C., AND ZARNEKOW, R. The value of community clouds for collaboration in the public sector. *Americas Conference on Information Systems* (2015).

[40] LAMBRINOUDAKIS, C., GRITZALIS, S., DRIDI, F., AND PERNUL, G. Security requirements for e-government services: a methodological approach for developing a common pki-based security policy. *Computer Communications 26* (10 2003), 1873–1883.

[41] LINS, S., SCHNEIDER, S., AND SUNYAEV, A. Trust is good, control is better: Creating secure clouds by continuous auditing. *IEEE Transactions on Cloud Computing 6* (8 2018), 1–14.

[42] LINS, S., SCHNEIDER, S., SZEFER, J., IBRAHEEM, S., AND SUNYAEV, A. Designing monitoring systems for continuous certification of cloud services: Deriving meta-requirements and design guidelines. *Communications of the Association for Information Systems 44* (8 2018), 1–49.

[43] MCKINSEY. Studie: Im öffentlichen Dienst fehlen bis 2030 140.000 IT-Fachkräfte, 2023.

[44] MELL, P., AND GRANCE, T. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. *National Institute of Standards and Technology 800* (2011), 1–7.

[45] NATALIE, Z. Studie zur Cloud-Nutzung : Wolken über dem Public Sector, 6 2024.

[46] NSA. Uphold the cloud shared responsibility model, 3 2024.

[47] PAQUETTE, S., JAEGER, P., AND WILSON, S. Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly - GOVT INFORM QUART 27* (8 2010), 245–253.

[48] PEFFERS, K., TUUNANEN, T., ROTHENBERGER, M., AND CHATTERJEE, S. A design science research methodology for information systems research. *Journal of Management Information Systems 24* (8 2007), 45–77.

[49] PINHEIRO JUNIOR, L., ALEXANDRA CUNHA, M., JANSSEN, M., AND MATHEUS, R. Towards a framework for cloud computing use by governments: Leaders, followers and laggers. In *Proceedings of the 21st Annual International Conference on Digital Government Research* (New York, NY, USA, 2020), dg.o '20, Association for Computing Machinery, p. 155–163.

[50] PWC. Fachkräftemangel im öffentlichen Sektor, 2022.

[51] REBOLLO, O., MELLADO, D., FERNÁNDEZ-MEDINA, E., AND MOURATIDIS, H. Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology 58* (2015), 44–57.

[52] RENNER, M., LINS, S., AND SUNYAEV, A. A taxonomy of is certification's characteristics. In *Proceedings of the 2021 2nd International Conference on Internet and E-Business* (2021), Association for Computing Machinery, pp. 1–8.

[53] SCHLARMAN, S. The People, Policy, Technology (PPT) Model: Core Elements of the Security Process. *Information Systems Security 10* (2001), 1–6.

[54] SCHNEIDER, S., AND SUNYAEV, A. Determinant factors of cloud-sourcing decisions: Reflecting on the it outsourcing literature in the era of cloud computing. *Journal of Information Technology 31* (8 2014), 2016.

[55] SEBASTIAN, L., STEPHAN, S., AND ALI, S. *Monitoring-basiertes Zertifizierungsverfahren*. Springer Berlin Heidelberg, 2019, pp. 189–222.

[56] SUBASHINI, S., AND KAVITHA, V. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications 34*, 1 (2011), 1–11.

[57] VICKY, IOANNIS, A. E. N., AND MANTHOU. Cloud computing adoption decision in e-government. In *Operational Research in the Digital Era – ICT Challenges* (2019), K. S. Angelo and Petridis, Eds., Springer International Publishing, pp. 125–145.

[58] WEGWEISER RESEARCH & STRATEGY. Im Spannungsfeld zwischen Innovation und Souveränität: Cloud und die digitale Zukunft der Verwaltung - Markt, Entwicklungsperspektiven und Entscheidungsstrukturen, 2024.

[59] ZAHARIA-RĂDULESCU, A.-M., AND RADU, I. Cloud computing and public administration: approaches in several european countries. *Proceedings of the International Conference on Business Excellence 11* (8 2017).

[60] ZWATTENDORFER, B., STRANACHER, K., TAUBER, A., AND REICHSTÄDTER, P. Cloud computing in e-government across europe : A comparison. In *Proc. of 2nd Joint International Conference on Electronic Government and the Information Systems Perspective, and Electronic Democracy, EGOVIS/EDEM* (8 2013), vol. 8061, pp. 181–195.