CLOUD CERTIFICATION TO FOSTER DIGITAL TRANSFORMATION MANAGEMENT IN PUBLIC ADMINISTRATIONS

Michael Diener
University of Regensburg and City of Regensburg, Germany
Felix Roessle
Technical University of Applied Sciences Rosenheim, Germany

Abstract

Public administrations are struggling with the adoption of cloud computing and face more severe challenges in the management than corporations due to special requirements regarding data protection and security. Certification of cloud services is the most promising method in overcoming the current issues. However, this paper examines that existing certificates for cloud service providers don't match the requirements of public administrations. The analyzed cloud certificates focus strongly on the information security management. But they only have a general look on data protection management. The missing focus on the special requirements of public administrations with regards to geo location of servers, the US cloud act, and especially prevention of foreign state access of PII data (personally identifiable information) is most critical for the use in public administrations. This article shows that a FedRAMP equivalent certification process combined with a European cloud certificate especially designed for the public administration could be the trigger to a successful and faster cloud implementation in the public administration sector in Europe that is currently underdeveloped. Furthermore, the large market with millions of buying public administrations in 27 European Union countries would create attractive business opportunities for private cloud providers, foster the development of new applications and serve the strategic goal of data sovereignty.

Keywords: Public administrations, adoption of e-Government, information security management

INTRODUCTION

Research topicality and problem. The rapid proliferation of cloud computing has transformed the delivery of IT services across various sectors, offering scalable, cost-effective, and innovative solutions for modern digital needs (Mell and Grance, 2011; Lin and Chen, 2012). However, public administrations in Europe face significant challenges in adopting cloud services, primarily due to stringent data protection and security requirements mandated by regulations such as the European General Data Protection Regulation (GDPR) (Altorbaq et al., 2017). Unlike private enterprises, public administrations must navigate complex legal frameworks, including concerns over data sovereignty and the risk of foreign state access to personally identifiable information (PII), as highlighted by the US CLOUD Act (Abraha, 2019). Existing literature indicates that while cloud certifications are critical tools for assessing cloud service providers (CSPs), they often fail to address the specific needs of public administrations, particularly regarding geo-location of data and prevention of unauthorized access (Schneider and Sunyaev, 2014; Lins et al., 2016). The scarcity of academic research on cloud adoption in the public sector underscores the urgency of investigating how certifications can bridge this gap, fostering secure and efficient digital transformation in public administrations.

The aim of the research. The aim of this study is to evaluate the applicability of existing cloud certifications for public administrations in Europe and propose a tailored certification framework to enhance cloud adoption. The research seeks to analyze the characteristics of current cloud certifications, identify their shortcomings in meeting public sector requirements, and recommend a certification model inspired by the US Federal Risk and Authorization Management Program (FedRAMP) combined with European-specific standards to ensure compliance with data protection and security needs.

Research methodology. The study employs a comprehensive analysis of 11 cloud certifications relevant to the European market, selected based on their focus on information security management and applicability to public administrations. Data were collected through an extensive review of academic databases, publicly available lists, and consultations with public administration experts, including data protection officers. The certifications were evaluated against eight key dimensions critical for public sector cloud adoption: information

security management, risk management, business continuity management, sub-service provider documentation, geo-location documentation, official investigation information processes, prevention of foreign state access, and data protection management. The analysis compares the fulfillment grades of these dimensions and examines governmental regulation initiatives, such as the EUCS and SecNumCloud, to assess their potential in addressing public sector needs.

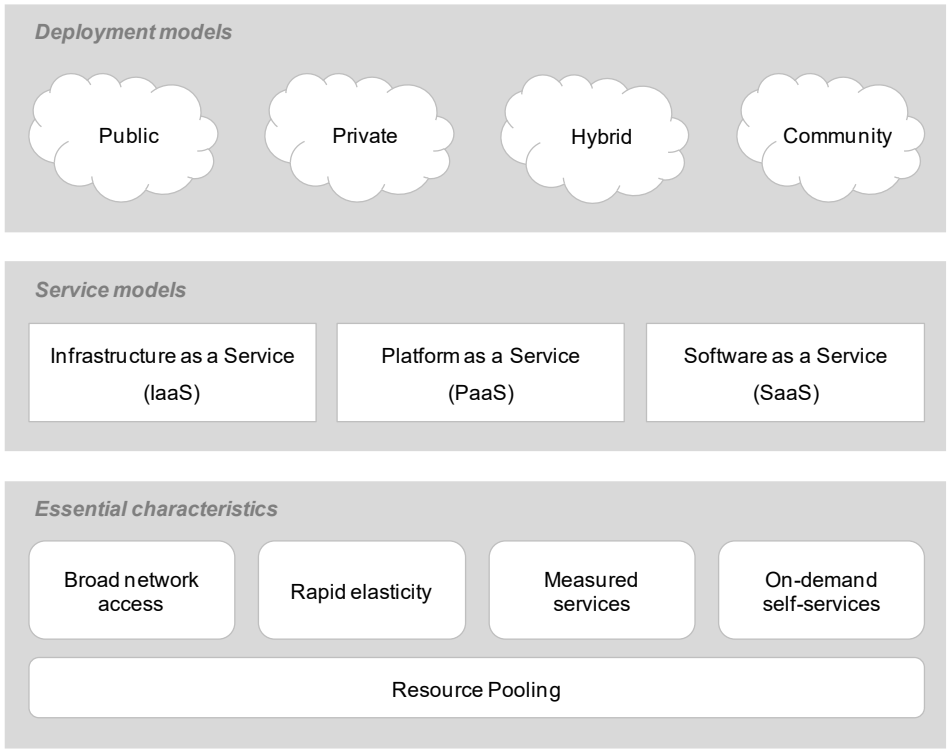
Research results. The findings reveal that while existing cloud certifications adequately address information security management, they often lack mandatory requirements for critical public sector needs, such as prevention of foreign state access and detailed geo-location documentation. Only four certifications partially address foreign state access, and none mandate it as a compulsory criterion. Governmental initiatives like the EUCS and SecNumCloud show promise in meeting these requirements, but challenges remain due to language barriers and limited transparency. The study proposes a FedRAMP-equivalent certification process tailored for Europe, combined with continuous auditing, to facilitate secure cloud adoption in public administrations.

Originality/Value of the article. This research is the first to systematically evaluate a comprehensive sample of cloud certifications with a specific focus on their applicability to European public administrations. By identifying gaps in existing certifications, particularly concerning data sovereignty and foreign state access, the study offers a novel perspective on the barriers to cloud adoption in the public sector. The proposed FedRAMP-inspired European certification framework provides a practical and scalable solution, enhancing trust and compliance in cloud services. The findings are valuable for policymakers, public administration IT managers, and CSPs, offering a pathway to accelerate digital transformation while ensuring regulatory compliance. Future research can explore the integration of dynamic auditing mechanisms and the role of initiatives like Gaia-X in creating a robust European cloud ecosystem, ensuring continuity and scalability of secure cloud solutions for public administrations.

RESEARCH METHODOLOGY

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). 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.

In general, IT departments do not need to own, maintain, or run the cloud infrastructure, platform, or application by themselves. The components are managed third-party companies (Ouedraogo and Mouratidis, 2013). The main advantages for outsourcing to a 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).



1 fig. US National Institute of Standards and Technology definition of cloud computing
Source: Compiled by the authors, based on US National Institute of Standards and Technology, 2025

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 EU. 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-centre 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 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 the cloud 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 considering 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 basically preventing 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 outsourcing parts or the entire IT processes to the cloud a complex process. 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 should a small community check whether Microsoft is following data privacy).

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 in the public sector. 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., 2022, 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 an entire CSP, there is temporarily a huge lack of transparency between the provider and the customer (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 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 analysed, 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 cloud provider, 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). 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. Therefore, it is necessary that decision makers in the public administration sector are aware of the differences in the available cloud certifications and have a clear guideline regarding the certificate that has to be used. When analysing 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 computing 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.

RESEARCH METHODOLOGY

Cloud certificates are the most promising method for leveraging cloud adoption in enterprises and public administrations. To investigate the applicability of existing cloud certificates for choosing a suitable cloud service and service provider in the public administration sector, we analyse 11 cloud certificates. This is the most comprehensive sample

of cloud certificates analysed 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 don't 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 were interviewing 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 analysed in depth scientific cloud adoption frameworks, underlying jurisdiction, cloud certification guidelines and public private research projects. Finally, one author of this paper is CISO at a large public administration.

To analyse 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 (annex 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 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. 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.

RESEARCH RESULTS AND DATA ANALYSIS

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

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. All certificates analyse 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.

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 of the involved partnerships. 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 a must have criterion. 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 centres, 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 for the public administrations, 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 data 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 in the context of cloud usage.

Finally, we investigate at the data protection management perspective of the analysed certificates. Only few tests 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 (annex 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 the public administration, 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.

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 solution. 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, 2022). As of today, there are more than 300 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 the FedRAMP is an aspirational target set-up to grow the use of secure cloud computing for the public administration sector in Europe.

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 public administrations (BSI, 2021), including very strict requirements, for instance regarding foreign state access. 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. Analysing 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 (annex 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 administration. 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. We 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.

We propose 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 analysed 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 analysed. Meanwhile, we propose conducting further research in analysing and designing a specific cloud requirement scheme that can be used temporarily by public administrations until the aforementioned Gaia-X solution is established.

CONCLUSIONS

1. The analysis of 11 cloud certifications reveals that while they comprehensively address information security management, they inadequately cover critical public administration requirements, such as the prevention of foreign state access to personally identifiable information (PII) and detailed geo-location documentation of data centers. Empirically, none of the certifications mandate prevention of foreign state access as a compulsory criterion, and only five certifications include geo-location documentation as a should-have requirement, highlighting a significant gap in meeting public sector needs.
2. Current cloud certifications provide robust frameworks for general information security but fall short in addressing the specific regulatory and operational constraints of public administrations, particularly concerning data sovereignty and transparency in sub-service provider documentation. The theoretical framework underscores the complexity of public sector procurement, which is constrained by strict regulations and the need for transparency. Empirical results show that certifications like the European Privacy Seal and BSI C5 partially address these concerns but are limited by factors such as private ownership of certification criteria or applicability to non-EU providers.
3. Governmental regulation initiatives, such as the European Cybersecurity Certification Scheme for Cloud Services (EUCS) and France's SecNumCloud, demonstrate significant progress in addressing public administration requirements by incorporating mandatory criteria for data protection, geo-location, and prevention of foreign state access. The theoretical basis highlights the need for standardized, transparent certification processes to foster trust and compliance. Empirically, these initiatives outperform existing certifications by fulfilling most critical dimensions, though challenges like language barriers and cross-referencing to local standards limit their broader applicability.
4. A FedRAMP-equivalent certification process tailored for Europe, combined with continuous dynamic auditing, is proposed as a viable solution to accelerate secure cloud adoption in public administrations. The theoretical literature supports the efficacy of centralized certification models like FedRAMP in reducing duplicative efforts and ensuring compliance (FedRAMP, 2022). The findings suggest that integrating such a model with European-specific standards, like EUCS, could create a transparent and scalable marketplace for pre-checked cloud services, enabling even small public administrations to adopt innovative solutions while adhering to stringent regulations.

LITERATURE

1. Abraha, H. (2019). How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis. *International Data Privacy Law, 9*(3), 207–215. https://doi.org/10.1093/idpl/ipz009
2. Abraham, A., Hörandner, F., Zefferer, T., & Zwattendorfer, B. (2020). E-government in the public cloud. *Electronic Government, an International Journal, 16*(3), 260–280. https://doi.org/10.1504/EG.2020.108455
3. Agarwal, A., & Agarwal, A. (2011). The security risks associated with cloud computing. *International Journal of Computer Applications in Engineering Sciences, 1*(Special Issue), 257–259.
4. Agostino, D., Arnaboldi, M., & Lema, M. (2021). New development: COVID-19 as an accelerator of digital transformation in public service delivery. *Public Money & Management, 41*(1), 69–72. https://doi.org/10.1080/09540962.2020.1764206
5. Ali, O., Shrestha, A., Ghasemaghaei, M., & Beydoun, G. (2022). Assessment of complexity in cloud computing adoption: A cross-sectional study of Australian organizations. *Information Systems Frontiers, 24*(5), 1607–1629. https://doi.org/10.1007/s10796-021-10108-w
6. Altorbaq, A., Blix, F., & Sörman, S. (2017). *Data subject rights in the cloud.* In 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 305–310). IEEE. https://doi.org/10.23919/ICITST.2017.8356406
7. Agence nationale de la sécurité des systèmes d'information. (2022). *Cloud computing service providers (SecNumCloud) requirements repository.*
8. 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

9. 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
10. Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Decision Support Systems, 52*(1), 232–246. https://doi.org/10.1016/j.dss.2011.07.007
11. Bundesamt für Sicherheit in der Informationstechnik. (2020). *Cloud computing compliance criteria catalogue*.
12. Bundesamt für Sicherheit in der Informationstechnik. (2021). *Mindeststandard des BSI zur Nutzung externer Cloud-Dienste*.
13. Bundesregierung, I.-B. (2022). *Bundescloud*. CIO.BUND.
14. Caudle, S. L., Gorr, W. L., & Newcomer, K. E. (1991). Key information systems management issues for the public sector. *MIS Quarterly, 15*(2), 171–188. https://doi.org/10.2307/249378
15. Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. In 2012 *International Conference on Computer Science and Electronics Engineering* (Vol. 2, pp. 647–651). IEEE. https://doi.org/10.1109/ICCSEE.2012.193
16. Dataguidance. (2021). *France government announces national cloud strategy*.
17. 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, 19*(2), 27–38. https://doi.org/10.21511/im.19(2).2023.03
18. Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: Issues and challenges. In 2010 24th IEEE *International Conference on Advanced Information Networking and Applications* (pp. 27–33). IEEE. https://doi.org/10.1109/AINA.2010.187
19. European Union Agency for Cybersecurity - ENISA. (2020). *European Union cybersecurity certification scheme for cloud services*.
20. Eurostat. (2021). *Percentage of companies with more than 10 employees in selected countries in Europe using paid cloud computing services*.
21. FedRAMP. (2022). *Securing cloud services for the federal government*.
22. 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, 25*(4), 808–835. https://doi.org/10.1080/14719037.2022.2037014
23. Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management, 28*(1), 107–130. https://doi.org/10.1108/JEIM-08-2013-0065
24. Garg, S. K., Versteeg, S., & Buyya, R. (2013). A framework for ranking of cloud computing services. *Future Generation Computer Systems, 29*(4), 1012–1023. https://doi.org/10.1016/j.future.2012.06.006
25. Gartner. (2021). *Cloud computing market research*.
26. Gholami, M. F., Daneshgar, F., Beydoun, G., & Rabhi, F. (2017). Challenges in migrating legacy software systems to the cloud - An empirical study. *Information Systems, 67*, 100–113. https://doi.org/10.1016/j.is.2017.03.008
27. Gholami, M. F., Daneshgar, F., Low, G., & Beydoun, G. (2016). Cloud migration process—A survey, evaluation framework, and open challenges. *Journal of Systems and Software, 120*, 31–69. https://doi.org/10.1016/j.jss.2016.06.068
28. Halabi, T., & Bellaiche, M. (2017). Evaluation and selection of cloud security services based on multi-criteria analysis MCA. In 2017 *International Conference on Computing, Networking and Communications* (ICNC) (pp. 706–710). IEEE. https://doi.org/10.1109/ICCNC.2017.7876216
29. Heidkamp, P., Vogel, M., & Gentemann, L. (2021). *Cloud-Monitor 2021*. KPMG and Bitkom Research.
30. Hon, W. K., Millard, C., & Walden, I. (2011). The problem of 'personal data' in cloud computing: What information is regulated?—The cloud of unknowing, Part 1. *International Data Privacy Law, 1*(4), 211–228. https://doi.org/10.1093/idpl/ipr018
31. ICT Market Experts. (2019). *Cooperation of the National Cloud Operator with Google Cloud*. https://ictmarketexperts.com/en/news/cooperation-of-the-national-cloud-operator-with-google-cloud/
32. Janssen, M., Rana, N. P., Slade, E. L., & Dwivedi, Y. K. (2022). Trustworthiness of digital government services: Deriving a comprehensive theory through interpretive structural modelling. In N. P. Rana, M. Janssen, Y. K. Dwivedi, & M. Weerakkody (Eds.), *Digital government and public management* (pp. 15–39). Routledge.
33. Khan, K. M., & Malluhi, Q. (2013). Trust in cloud services: Providing more controls to clients. *Computer, 46*(7), 94–96. https://doi.org/10.1109/MC.2013.254
34. Krotsiani, M., Spanoudakis, G., & Kloukinas, C. (2015). Monitoring-based certification of cloud service security. In *On the Move to Meaningful Internet Systems: OTM 2015 Conferences* (pp. 644–659). Springer. https://doi.org/10.1007/978-3-319-26148-5_44
35. Kuhlmann, S., & Heuberger, M. (2023). Digital transformation going local: Implementation, impacts and constraints from a German perspective. *Public Money & Management, 43*(2), 147–155. https://doi.org/10.1080/09540962.2021.1939584

36. 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. In *eChallenges e-2014 Conference Proceedings* (pp. 1–10). IEEE.
37. Lang, M., Wiesche, M., & Krcmar, H. (2016). What are the most important criteria for cloud service provider selection? A Delphi study. In *Proceedings of the Twenty-Fourth European Conference on Information Systems* (ECIS).
38. Lang, M., Wiesche, M., & Krcmar, H. (2018). Möglichkeiten zum Nachweis vertrauenswürdiger Cloud-Services. In A. Sunyaev, S. Schneider, & M. Wiesche (Eds.), *Management sicherer Cloud-Services* (pp. 59–68). Springer. https://doi.org/10.1007/978-3-658-19579-3_5
39. Lember, V., Brandsen, T., & Tõnurist, P. (2019). The potential impacts of digital technologies on co-production and co-creation. *Public Management Review, 21*(11), 1665–1686. https://doi.org/10.1080/14719037.2019.1619807
40. Lin, A., & Chen, N.-C. (2012). Cloud computing as an innovation: Percepetion, attitude, and adoption. *International Journal of Information Management, 32*(6), 533–540. https://doi.org/10.1016/j.ijinfomgt.2012.04.001
41. Lins, S., Grochol, P., Schneider, S., & Sunyaev, A. (2016). Dynamic certification of cloud services: Trust, but verify! *IEEE Security & Privacy, 14*(2), 66–71. https://doi.org/10.1109/MSP.2016.26
42. Lins, S., Schneider, S., & Sunyaev, A. (2021). Trust is good, control is better: Trusted cloud computing providers. *IEEE Transactions on Cloud Computing, 9*(3), 890–903. https://doi.org/10.1109/TCC.2016.2522411
43. 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, 18*(3), 93–105. https://doi.org/10.21511/ppm.18(3).2020.08
44. 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, 15*(6–7), 2059–2063. https://doi.org/10.1166/jctn.2018.7407
45. Margetts, H., & Willcocks, L. (1993). Information technology in public services: Disaster faster? *Public Money & Management, 13*(2), 49–56. https://doi.org/10.1080/09540969309387763
46. 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*. https://www.marketsandmarkets.com/
47. Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing (NIST Special Publication 800-145)*. National Institute of Standards and Technology.
48. Moe, C. E. (2014). Research on public procurement of information systems: The need for a systematic approach. *Communications of the Association for Information Systems, 34*(1), Article 78. https://doi.org/10.17705/1CAIS.03478
49. Moe, C. E., Newman, M., & Sein, M. K. (2017). The public procurement of information systems: Dialectics in requirements specification. *European Journal of Information Systems, 26*(2), 143–163. https://doi.org/10.1057/s41303-017-0035-4
50. NEN. (2021). *Baseline information security government*. Stichting Koninklijk Nederlands Normalisatie Instituut.
51. Opara-Martins, J., Sahandi, R., & Tian, F. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. *Journal of Cloud Computing, 5*(1), Article 4. https://doi.org/10.1186/s13677-016-0054-z
52. Ouedraogo, M., & Mouratidis, H. (2013). Selecting a cloud service provider in the age of cybercrime. *Computers & Security, 38*, 3–13. https://doi.org/10.1016/j.cose.2013.01.007
53. Piswanger, C.-M., & Strick, L. (2017). European innovation procurement "Pre-Commercial-Procurement" and cloud computing by reference to the research project "Cloud for Europe". In 2017 *Fourth International Conference on eDemocracy & eGovernment (ICEDEG)* (pp. 161–166). IEEE. https://doi.org/10.1109/ICEDEG.2017.7962527
54. 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, 13*(3), 213–222. https://doi.org/10.1049/iet-sen.2018.5293
55. Rojszczak, M. (2020). CLOUD Act agreements from an EU perspective. *Computer Law & Security Review, 38*, Article 105442. https://doi.org/10.1016/j.clsr.2020.105442
56. Rutherford, M. (2019). The CLOUD Act: *A primer for non-US privacy professionals*. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3508942
57. Saraswat, M., & Tripathi, R. C. (2020). Cloud computing: Security issues and challenges. In 2020 *9th International Conference System Modeling and Advancement in Research Trends (SMART)* (pp. 281–285). IEEE. https://doi.org/10.1109/SMART50582.2020.9337100

58. Schneider, S., & Sunyaev, A. (2014). Determinant factors of cloud-sourcing decisions: Reflecting on the IT outsourcing literature in the era of cloud computing. *Journal of Information Technology, 31*(1), 1–31. https://doi.org/10.1057/jit.2014.25
59. Schwartz, P. M., & Peifer, K.-N. (2019). Data localization under the CLOUD Act and the GDPR: Transatlantic conflicts and solutions. *Computer Law Review International, 20*(1), 1–10. https://doi.org/10.9785/cri-2019-200102
60. Seo, J., Min, J.-S., & Lee, H. (2014). Implementation strategy for a public service based on cloud computing at the government: Case study for Korea. *International Journal of Software Engineering and Its Applications, 8*(9), 207–220. https://doi.org/10.14257/ijseia.2014.8.9.17
61. 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, 25*(4), 710–733. https://doi.org/10.1080/14719037.2022.2033052
62. SPD, Bündnis 90/Die Grünen, & FDP. (2021). *Mehr Fortschritt wagen: Koalitionsvertrag 2021–2025.*
63. Subramanian, G., Patil, B. T., & Gardas, B. 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, 16*(3), 944–962. https://doi.org/10.1108/JM2-08-2020-0207
64. Sullivan, M. (2022). *Public sector cloud adoption: Don't just adopt cloud computing, adapt to it*. Deloitte. https://www2.deloitte.com/xe/en/insights/industry/public-sector/public-sector-cloud-adoption.html
65. Sunyaev, A., & Schneider, S. (2013). Cloud services certification: How to address the lack of transparency, trust, and accountability in cloud computing. *Communications of the ACM, 56*(2), 33–36. https://doi.org/10.1145/2408776.2408789
66. Tang, C., & Liu, J. (2015). Selecting a trusted cloud service provider for your SaaS program. *Computers & Security, 50*, 60–73. https://doi.org/10.1016/j.cose.2015.02.001
67. Walker, K. (2016). *CSA releases cloud computing top threats in 2016*. Cloud Security Alliance.
68. Zaharia-Rădulescu, A.-M., & Radu, I. (2017). Cloud computing and public administration: Approaches in EU countries. *Proceedings of the International Conference on Business Excellence, 11*(1), 739–749. https://doi.org/10.1515/picbe-2017-0078
69. Zwattendorfer, B., Stranacher, K., Tauber, A., & Reichstädter, P. (2013). Cloud computing in e-government across Europe: A comparison. In *Technology-Enabled Innovation for Democracy, Government and Governance* (pp. 181–195). Springer. https://doi.org/10.1007/978-3-642-40160-2_15

Annex 1

Table 1. Summary statistics of cloud certificates

Certificate	Provide	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	CSPs	1
BSI IT-Grundschutz	BSI	Government	1994	Feb 22	IS	National Standard	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

Source: compiled by the authors, 2025

Annex 2

Table 2. Cloud certificates fulfilment grade for public administration requirements

Certificate	ISM	RM	BCM	Sub service provider	Geo location documentation	Official investigation information	Prevention of foreign state	Data protection management
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	✓✓

Table information: This table presents the cloud certificates and the fulfilment grade of relevant characteristics, 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.
Source: compiled by the authors, 2025

Annex 3

Table 3. Cloud certificates fulfilment grade for public administration requirements

Certificate	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.

Source: compiled by the authors, 2025