

On Challenges of Cyber and Information Security Management in Federal Structures - The Example of German Public Administration

Thomas Rehbohm¹, Kurt Sandkuhl^{1,4}, Thomas Kemmerich^{2,3}

¹ Institute of Computer Science, University of Rostock, Germany

² Technologie-Zentrum Informatik und Informationstechnik, University of Bremen, Germany

³ Norwegian University of Science and Technology, Trondheim, Norway

⁴ Jönköping University, Jönköping, Sweden

Abstract. Security management in organizations is a complex task requiring defined organizational structures and processes. Established standards and recommendations provide methodological guidance for establishing and managing security. However, it has been observed that governmental or public bodies show different challenges in security management than industrial organizations due to their often densely regulated settings. In this context, in particular federal multi-layered structures have been pointed out as hard to manage. The main contributions of this paper are the results of an interview study among the chief information and security officers (CISOs) of the federal states of Germany. The results shed light on current challenges in cybersecurity management. The results are meant to establish the relevance of research work in this area and to be the starting point of developing artefacts or instruments supporting cybersecurity management at the interface of federal states and municipalities in particular.

Keywords: Reference model, cyber security, public administration.

1 Introduction

Security management in organizations is a complex task requiring defined organizational structures and processes and encompassing various aspects, such as technology, culture, competency, documentation, etc. [4]. Established standards and recommendations, as for example ISO 27001 [1], SABSA [2] or IT Grundschutz [3], provide methodological guidance for establishing and managing security. However, it has been observed that governmental or public bodies show different challenges in security management than industrial organizations due to their often densely regulated settings. In this context, in particular federal multi-layered structures have been pointed out as hard to manage. This paper aims at contributing to a better understanding of the organizational and policy-related challenges of implementing cybersecurity management in federal states based on the example of Germany.

Taking the relationship between the federation, federal states and municipalities as focus area, the paper investigates the perceived challenges of policy implementation

Copyright © 2019 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0)

on executive level in the states from a governance perspective. More concrete, the study investigates the view of the CISO within an interview study.

Although our work investigates challenges for management of cyber and information security in German public administration only, there are indications of previous work that similar challenges are also visible in other federal structures. For example, [6] analyzed and compared practices in cybersecurity implementation in the US, Germany and China, and concluded the need for detailed analysis work.

The information and cyber security of the public administration at federal, state and local level is determined by many factors. Germany's federal system is subject to dependencies comparable to those of Europe in relation to its member states. All public administrations face the same challenges as citizens and businesses. Information and cyber security is threatened and can only be ensured with increased use of technical and human resources. In addition, the political will must exist and legal conformity must be established. The technical infrastructures of the administrations are an essential basis for government services for citizens and society. Therefore, the resilience of companies providing services of general interest - including the public sector - in the administrative structure must be ensured. Information security of the public administration therefore has to include all relevant aspects of cyber security.

Cyber and information security is not a question of national or federal administrative structures. The legislation and the associated rights and obligations must be determined by uniform possibilities of action against highly dynamic - also criminal - actors on the Internet. This problem is to be investigated in an interview study as part of this work. The specific aspects of IT management in the administrations and their internal structure in Europe, the German Federal Government, the Federal States and local authorities will be identified and approaches to solutions will be developed. Possibilities for the collection of data arise in the federal states' working committees of the Conference of the Interior Ministers and the IT Planning Council.

Despite certain coordination attempts by the German IT Planning Council, the digitisation of the administration also takes place according to the strategy of the federal state and local authority. Due to this form of digitisation in Germany in general and in the administrations in particular, the efforts of comparable and uniform information security management at all levels of government in Germany will be given lower priority. In comparison to the private economy, the administrations have no overriding requirements for the implementation of information technology content objectives, an inherent problem of the system. The public administrations are not only responsible for their own IT and the digitalisation of administrative services, but also for the critical infrastructure. With the federal legal requirements on critical infrastructures, the federal states have at least moved into the focus of IT situations in the area of existence prediction. In the meantime, it has also become apparent that purely arithmetically recorded companies of general interest do not cover the target group of major cities and regions.

From a political perspective, the federal government, the separate governments of the federal states and the various municipality councils are in charge of implementing EU laws and regulations or transposing into national law or directives. From an executive perspective, i.e. implementation of the political will manifested in the legisla-

tion, the federal states and their organization structures play an important role, as they are in charge of guiding, directing and supervising the subordinate agencies or administrations in their federal state. In this context, the CISOs of the federal states are the central roles (cf. section 2 and 4).

The main contributions of this paper are the results of an interview study among the CISOs of the federal states of Germany. The results shed light on current challenges in cybersecurity management. They are meant to establish the relevance of research work in this area and to be the starting point of developing artefacts or instruments supporting cybersecurity management at the interface of federal states and municipalities in particular.

The remaining part of the paper is structured as follows: Section 2 introduces background information on public sector data protection in federal structures. Section 3 introduces the research methodology applied in the paper. Section 4 summarizes the results of a literature study. Section 5 presents design and results of the interview study performed among the CISOs. Section 6 summarizes the findings and implications for future work.

2 Public sector data protection in federal structures

The information and cyber security of the federal, state and municipal public administrations is determined by many factors. Germany's federal system is subject to dependencies comparable to those of Europe in relation to its member states. Public administrations commonly face the same challenges in cyber security as citizens and businesses. Information and cyber security is threatened and can only be ensured with increased use of technical and human resources. In addition, the according political will must exist and legal conformity must be established.

The technical infrastructures of administrations are an essential basis for government services for citizens and society. Therefore, the resilience of companies providing services of general interest - including the public sector - must be ensured in the administrative division of Germany. The information security of the public administration is to be extended thus by the aspects of the cyber security.

In the literature, the topic of technology and "data protection impact assessment" of the critical infrastructure "public administration" and its information technology with regard to ensuring information and cyber security has not yet been dealt with in a structural approach. Only partial aspects of the respective responsibilities of the ministries at federal and state level are subject to closer scientific examination.

The Committee for Education, Research and Technology Assessment in the Bundestag, for example, dealt with the "endangerment and vulnerability of modern societies - using the example of a large-scale and long-lasting power failure" and its effects on society's telecommunications and information technology [6].

"The impact analyses have shown that after only a few days it is no longer possible to ensure the nationwide supply of the population with (vital) necessary goods and services in the affected area. Public security is at risk, and the state can no longer meet the constitutional obligation to protect the life and limb of its citizens. In doing

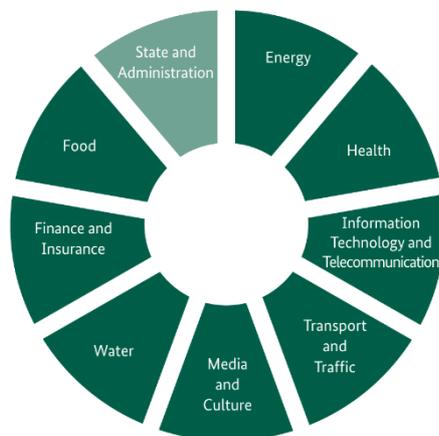
so, it would also lose one of its most important resources - the trust of its citizens". (Committee on Education, 2011)

This result does not go far enough for the consideration envisaged in this paper, but shows that even a power failure with a low probability of occurrence - across state borders - would be tantamount to a national catastrophe.

As a result of such investigations, the federal government has renewed the implementation plans for critical infrastructures and the federal government. The sectors (Figure 1) energy, food, finance and insurance, health, information technology and telecommunications, media and culture, transport and traffic as well as water are addressed via the UP Critis, the state and administration via the UP Bund. The Federal Office for Civil Protection and Disaster Relief is responsible together with the Federal Office for Information Security and pursues the following objectives:

- Promotion of the robustness of ICT components in critical processes
- Exchange on current incidents
- Joint assessment and evaluation of the cyber security situation
- Development of common documents and positions
- Establishment and expansion of crisis management structures
- Coordinated crisis response and management
- Conducting emergency and crisis exercises
- Joint action vis-à-vis third parties

Within the framework of the legislative competence of the federal government, these objectives are supported at several legal levels. The Act to Increase the Security of



Information Technology Systems (IT Security Act) - as an Article Act - applies to most of the aforementioned sectors and obliges operators of such infrastructures to take special measures, coordinated with the Federal Office for Information Security (BSI), to increase resilience to cyber attacks.

The "state and administration" sector is only indirectly affected by federal regulations, as the sector cannot be legally addressed due to federal responsibilities and is provided for in the UP Bund. This scientific work should start with the effects.

Figure 1 Critical infrastructure sectors in Germany

The federal government and the federal states have set up various working groups for the topics of information security and cyber security with conditionally coordinated work contents. Different departments for reasons of competence also staff them:

- A working group chaired by the Conference of Interior Ministers (IMK) is dealing with the issue of cyber security. A scientific discussion under a holistic approach is to take place - governed by the National Cyber Security Council (NCSR) - the permanent working group of the IMK has been established as the working level of the NCSR. The NCSR is composed of political leaders and business representatives, bundles the activities for cyber security between state and business and is coordinated by the Federal Government Commissioner for Information Technology.
- The information security concerns of the Federal Government and the federal states are coordinated in a permanent working group of the IT Planning Council (IT State Treaty on the Establishment of the IT Planning Council). Representatives from various departments are delegated to this working group.

In 2009, the Federalism Commission II created the basis for binding IT coordination between the federal and state governments with Article 91c of the Basic Law, i.e. constitution of the Federal Republic of Germany.

At European level, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security of network and information systems in the Union (NIS Directive) was adopted. As in the IT Security Act, the scope of "State and Administration" was not dealt with here either. The Act to Implement the Directive (EU) 2016/1148 of the European Parliament and the Council, the IT Security Act and the BSI Act with corresponding BSI Crisis Ordinances are merely the national legal implementations of the EU Directive and can therefore not close this gap.

3 Research Methodology

The main research methodologies used in this paper are literature research and interview study. The literature search (presented in section 4) aims at analyzing relevant related work in the scientific body of knowledge. One conclusion from this research is the lack of knowledge about the view of the federal states regarding the challenges of cybersecurity implementation. Thus, it was decided to perform an interview study among the CISO and analyze interview contents based on qualitative content analysis. The research question for the study performed is: *On the executive level of the federal states of Germany, what are the perceived status and expressed challenges of cybersecurity management?* "Executive level" in this context means that we include only the CISOs of the federal state in the study.

The research question is then further defined with an analysis of the content - the determination of the relevance of the topic - and the theoretical introduction into the research field.

A study in the form of guideline-supported interviews was carried out in order to define the topic area. Participants were the IT security officers of the federal states. The colleagues, also known as CISOs, described the challenges, opportunities and risks of their activities in an interview with defined questions. The interview guideline is the result of preliminary considerations, theoretical studies and maturity models developed in the past. The results obtained and written on were subjected to a qualita-

tive content analysis according to Phillip Mayring [7]. This method serves the purpose of empirical data evaluation and includes recommendations for a systematic and verifiable text analysis.

Mayring's approach [8] includes 6 steps: Step 1 is to decide what material to analyze, which consists in our case of the notes taken during the interviews. The interviewed CISOs all are experienced in the field of cybersecurity and qualified for their positions, which makes them suitable sources and experts for the research question. Step 2 is to make explicit how the data collection (i.e. in our case the interviews) was arranged and prepared. The purpose of this step is to make all factors transparent which could be relevant for interpreting the data. The CISOs were selected based on their position and from existing contacts of the researchers involved. As preparation for the interviews, the hypotheses and interview guidelines were arranged. The interviewees received information about the purpose of the interview. The interviews with the CISOs were between 28 and 56 minutes long.

Step 3 is to make explicit, how the transcription of the material had to be done. The material was analyzed step by step following rules of procedure devising the material into content analytical units. The rules included what IDs to use for the units of different interviews, how to tag content related to the interviewer and content from the interviewees, how to mark comments, etc. Step 4 concerns the subject-reference of the analysis, i.e. that the connection to the concrete subject of the analysis is made sure. Subject-reference was implemented by (a) defining the research question and corresponding sub-questions in the interview guidelines and (b) using the subjects of these sub-questions as categories during the analysis.

Step 5 recommends theory-guided analysis of the data, which is supposed to balance vagueness of qualitative analysis with theoretical stringency. For theory-guidance, we took the state-of-the-art into account during both, formulation of the sub-questions and analysis of the material. Step 6 defines the analysis technique, which in our case was content summary. This attempts to reduce the material in such a way as to preserve the essential content and by abstraction to create a manageable corpus which still reflects the original material.

All in all, the qualitative research focuses on the understanding of interrelationships, which is done here by means of interviews. This means, an inductive approach, which is concluded from empirical individual observations on the general. Quantitative research, on the other hand, is usually based on a questionnaire structure, with closed questions and given answer possibilities, as in the preliminary studies collected by the maturity models. Contexts are worked out and hypotheses tested. A deductive approach means, from the general to the specific. In a further step of the research, the questionnaires are to be carried out with a more extensive group of addressees.

4 Literature Analysis

Relevant literature for the topic under consideration was identified by using Google Scholar as the main search tool. Due to the nature of the topic, it quickly became obvious that many of the relevant sources were publications in German. The

available literature on this topic includes essential articles from the field of government and administration, which are mainly published in the context of German administrations. In addition, there are current developments from European research activities.

The article "Cyber security in critical infrastructures, European and German regulation - an overview" [9] deals with the connections between European and national regulation. In particular, the cooperation of the member states and the operators of infrastructures of general interest and their obligation to exchange information (reporting obligations) via central contact points. The federal states have established their own federal state CERTs (Computer Emergency Response Teams) for this purpose. Operators of critical infrastructures can also set them up, but are only obliged to have a single point of contact for receiving information and for reporting incidents. The joint exercises will also be conducted in the European area, which will now also play an important role at the national level.

Analogous to the Lükex (state and interdepartmental crisis management exercise) - controlled by the Federal Office for Civil Protection and Disaster Relief - states such as Hessen design special IT crisis management exercises (KRITEX) to deepen interdepartmental cooperation in the event of critical cyber events.

In the article "Security-Management-as-a-Service" [10], a problem is addressed which found in the meantime be identified in the entire German administrative structure, the lack of skilled workers. Another aspect is the fundamental affinity of IT employees with regard to awareness of cyber security risks, but there is a lack of holistic control of the security management process and a commitment to responsibility:

"Our investigations and in-depth interviews in several authorities throughout Germany gave a detailed but heterogeneous picture of the infrastructure used, the knowledge and motivation of the employees in the areas of IT security and security management, as well as the available personnel and financial resources." (Stefan Pfeiffer, 1/2019)

The administrations in Germany are structured in such a way that - as in the past decades - they can only recruit skilled workers with salaries and collectively agreed wages in areas that are specific to vocational training (traditionally according to vocational or academic qualifications). Unless rapid civil service is identified as a unique selling point of the administration, the administration must face up to the competition from commercial enterprises. Where administrations can overcome the proven systems of employee recruitment, a co-appointment between administrations of federal, state and local authorities (cannibalisation) is additionally created. A new way of recruiting employees and retaining them in the company, as well as employer branding, can only be expected in the future.

In the article "IT security - a law-free space" [11], the authors discuss the need to create further regulations; analogous to the basic data protection regulation, a basic IT security regulation should be created. This is based on the idea that IT security is a basic prerequisite for digital sovereignty. Digital sovereignty is understood to be multidimensional, to develop key technologies itself and to exercise control and self-determination over actions in the digital space. The evaluation from the interviews of this work resulted in a similar assessment. The Karlsruhe Institute of Technology, the

FZI Research Center for Computer Science and the Fraunhofer Institute for Optronics, Systems Engineering and Image Evaluation [12] investigated the complexity of the ideas about digital sovereignty in Europe. Important definitions of the understanding of digital sovereignty were also developed for this research.

“Infrastructure sovereignty refers to the ability to establish or verify the trustworthiness of technical infrastructures and to operate them in such a way that services offered thereon can be trusted. Data sovereignty refers to the ability to inform and decide for oneself how and by whom information about one's own person or institution, one's own actions or products is collected, processed and passed on. Decision sovereignty refers to the possibility of tracing the origins and justifications for decisions and recommendations for action of autonomous systems and assistants and, if necessary, influencing them by human intervention. Platform sovereignty arises when the market power of major players in a platform economy is limited to a degree where fair competition remains possible through regulation and conscious customer decisions.” (Jürgen Beyerer, 5/2018)

The above mentioned definitions are used in this work. The Karlsruhe Theses themselves and open research questions establish a motivation to investigate the topic of this work.

In "Systematization of IT Security Law" [13] the authors see an discrepant, incomprehensible and thus inconsistent IT legislation. The review begins with the 1990s; the first BSI laws, the data protection law, the signature law and the liability law. It is shown that since then the IT legislation has strongly diversified and in the following years, more than 60 legally effective regulations in the IT security environment arose at the federal government alone. From the area of critical infrastructures, special legal regulations were added, such as from the areas of energy, nuclear industry or telecommunications, which were last adapted in 2016 with the Article Law on IT Security (IT-SiG). Furthermore, shortcomings in the timely implementation of European legislation into German law are pointed out.

The European Parliament, the Council and the European Commission have reached political agreement on the legal act on cyber security at the end of 2018. It strengthens the mandate of the European Union Agency for Network and Information Security (ENISA). Resources will be pooled at ENISA to better help Member States deal with cyber security threats and attacks. A common cyber security certification will also be introduced. European Parliament passed the Cybersecurity Act in March 2019.

The "Case study-based analyses of IT security in critical infrastructures" [14] are an illustrative practical example. Particular attention was paid to critical infrastructures only after the Stuxnet incident (malware for Supervisory Control and Data Acquisition). However, the infiltration of industrial control systems was only the beginning. Private households, public administration or even hospitals are attacked in a targeted and non-targeted manner.

The case studies were based on guided expert interviews. A qualitative content analysis according to Mayring [7] evaluated the data according to their significance. Codes, such as the assessment and measurement of IT security, the enhancement of IT security, the simplicity of the measure or the cost efficiency of the measure, were formed and subjected to a cross case analysis in order to filter out similarities and

differences. The study serves the understanding of the complex connections of IT security projects and is suitable for the development of new research questions.

5 Interview Study

Based on the results of the literature study, it can be concluded that the existing publications cover the general situation in cybersecurity regulation in Germany and between Germany and the EU, but there is a lack of information about the political, strategic and technical challenges arising from managing cybersecurity on the federal state level. Thus, we decided to conduct an interview study involving the top executive level in the federal states. Section 5.1 describes the hypotheses underlying our work, section 5.2 discusses the procedures applied for performing the interview study and section 5.3 summarizes the results.

5.1 Hypotheses

Based on the literature work in sections 2 and 4, we define two hypotheses which are subject to investigation in the interview study.

Hypothesis 1: The management of information security and cyber security is carried out in a fragmented structure of responsibilities at federal and state level. The Federal Government mainly maps the links to Europe. The states are not established and in demand as designers of information and cyber security management.

Hypothesis 2: Although it is their intended role in the federation, the federal states do not act as driving forces shaping the cyber security of their municipalities - partly because of the municipal right of self-determination. This is aggravated by the obligation of the federal states to be connected (the relationship between the federal states and the municipalities is a legal principle that establishes legally enforceable claims by the municipalities against the federal states if they enact laws that have financial consequences for their municipalities). Only the central municipal associations can be identified here as further possible participants and co-designers. The Deutscher Landkreistag (DLT) has a coordinating function for the Deutscher Städtetag (DST) and the Deutscher Städte- und Gemeindebund (DStGB). Accordingly, the associations in the respective federal states are listed below.

Coordinating information and cyber security is a challenge given in the above-mentioned federal structures, inconsistent responsibilities and financial dependencies. This work will be the subject of a scientific study on the resilient structures of cooperation.

5.2 Procedure

The guideline-based interviews conducted in this study were based on the premise that information and cyber security are subject to political, strategic, technical and legal dependencies. In all cases, the interview partners were the CISOs of the federal states of Germany. The role of the information security officer of a federal state has been established as a functional office (Role of Information Security Management

System (ISMS)), which is usually located in the hierarchy of a ministry. Due to the special importance of the topic of information security, all CISOs have a direct right to speak to the head of the authority, the state secretary or the minister, and have also arranged regular meetings. As a rule, CISOs are career civil official or employees who, depending on their position in the respective ministry, also possess a corresponding qualification such as, jurists, engineers, natural scientists or corresponding qualification in the fields of law.

Two examples of questions from each of the four areas are given below for the lead question-supported interviews.

Political: How do you see the digital sovereignty of your federal state in the future?
What competencies and mandates does your ISMS and the CISO have?

Strategical: How "broad" is the scope of responsibility of the "information security management system" organization in your federal state (cyber vs. information security)?

Why do they (not) see IT as a strategic tool or would they also give up competences?

Technical: How do they view virtualisation on the internet and its use by their federal states (cloud)?

Which systems are used for active attack detection?

Legal: Where do you see regulatory deficiencies in your federal state?

How do they ensure compliance requirements for cloud usage variants?

In the course of the guideline-based interviews, the questions did not have to be used chronologically or entirely. Rather, in the course of the discussion it emerged that the contents desired by this work were addressed in full by the interviewees themselves.

5.3 Results

After evaluating the transcripts of the interviews, identical answers or identical tendencies were assigned to the statements of a group and were thus taken into account. Similarities, contradictions and differences were identified. Strongly differing statements were not taken into account for reasons of resilience or were suitable for elimination, especially tendentious statements. The official or personal circumstances of each interviewee were taken into account.

The results of the interviews are that both hypotheses were confirmed. The core results can be aggregated as follows:

a) Political perspective:

The concerns of the CISOs can be addressed on an adequate hierarchic level in the management (ministerial level) and are in part also regulated by law; this also applies beyond relevant safety incidents that are effective for the public.

The resources of information security management are predominantly acquired centrally and are responsible decentrally (departmental sovereignty). To date, no federal state has been able to establish a system of indicators for the effectiveness or improvement process of security management. "Key Performance Indicators" are defined by the federal states as a Request and are to be included in the annual reports.

Conformity with the respective national budget regulations is given, but no proof of a "return on investment" can be offered.

The respondents have different interpretations of the topic of digital sovereignty. As shown in the literature research, the CISOs want scope for action for different aspects of sovereignty (infrastructures, data, decisions or platforms). The concentration on a few central and "state-owned service providers" was the main focus of all respondents.

In the federal structures of the federal states in internal relations, no special mandates or competences were transferred to the CISOs or the central security management - over and above the rights in coping with emergency situations. The procedures are based on guidelines of the respective administration that are capable of compromise or consensus.

b) Strategic perspective

All central security management systems are consistently linked to ministerial authorities, if necessary with the Chief Information Officer (CIO) or the Chief Digital Officer (CDO) of the respective federal state. As a rule, the responsibility for cyber security does not lie within the information security management; in the classical structure of administrations, this topic can be found with civil protection/crisis management or with the state criminal investigation offices of the interior departments. Consequently, responsibility for commercial enterprises (critical infrastructures) is not linked to information security management either. The same applies to classic data protection, which is provided for by law and set up in independent authorities of its own. An exchange of content takes place via the working levels. Apart from the conflicting goals of information security and data protection (value protection vs. data protection), however, a common risk process has been formulated as a requirement.

IT and information security management is seen as a strategic means of achieving efficiency gains, i.e. the modernisation of administration and digitisation. Decision-making authority over IT and IT security is becoming a monopoly of power.

The municipalities are currently only rudimentarily involved in the IT (security) management processes. Local self-government has so far been little involved in the strategic planning of the federal states, although the special role of the municipalities as initiators of digitisation is clear.

c) Technical perspective

Technically, IT of public administration is far behind the state of the art. The existing classical systems and infrastructures have been developed along the requirements of the past decades. Newer technologies, for example for active attack detection, are only occasionally tested because they require a legal basis. The first federal states have made improvements here. Although respondents were aware of the enormous importance of cloud computing or artificial intelligence (AI) applications, there is only a limited willingness to exploit this potential. In very few federal states, there is a resilient strategy for use of cloud services; in addition, respondents see too many parties involved in the procedure, so that they are not prepared to do anything in advance.

d) Legal perspective

In many federal states there are legally binding regulations on information security in addition to data protection and the respondents mainly see implementation deficits

here. Cyber security aspects have so far not been addressed, nor have municipal aspects. In all federal states, there is a need to clear the backlog, starting with the critical infrastructures of the community (state and economy) up to municipal suppliers and the municipalities themselves.

There are sporadic legal bases in the federal states for the intervention in telecommunications secrecy, which is necessary for resilience against cyber attacks, in particular for breaking encrypted communication connections. The interviewees in the federal states consider national legislation in the federal government to be effective, whereas European legislation is too vague and federal state legislation creates inconsistencies. There is no legal basis for the use of cloud services; rather, the federal states rely on traditional mechanisms of audits along frameworks or federal guidelines, such as the BSI's Cloud Computing Compliance Controls Catalogue (C5).

6 Conclusions

The survey on information security carried out identified challenges and perspectives on the level of CISO and contributes to scoping future research in the field. No study before had access to the view of the CISOs of federal states of Germany which makes the study and its results unique. In particular, the evaluation using the maturity model showed that only the federal states are in a position to achieve above-average results, in which strategic and political intentions - explained via the change process in IT management - and measures were taken, which in turn have technical and legal consequences. Resource management in the respective institutions is of decisive importance. Both financial resources made available and availability of skilled personnel represent influences to be taken into account in all the dependencies considered.

The core result of our study is that there is a need for more specific instruments in coordinating the federation and the federal state level. Such instruments should exceed the support level offered by policies or guidelines and rather offer normative or best practice recommendations. In particular, we believe that a reference model covering organizational, application and information, and technology oriented aspects and at the same time showing how existing legislation is implemented, could be of significant value to the CISOs. Thus, future work will investigate both pertinence and feasibility of reference models and their development.

The presented study refines or condenses the result in such a way that further aspects of federal cooperation must be examined more closely. In addition, there is an extended focus on cyber security. Information security - maturity model - must be considered together with cyber security. Furthermore, an additional study is to determine which companies in the counties - and which measures - need to be supported by the federal states. Such dependencies should also be examined for the "state and administration" sector.

In research, IT has played a subordinate role in government and administration. The functioning of public infrastructures is of enormous importance for services of general interest. Interdependencies with other critical sectors were - if at all - insufficiently considered.

The further research will investigate the conflicts and deficits identified here, create a model a reference and evaluate the context in the federal, state and local governments. The results of this preliminary study must be taken into account.

The reference model must do justice to the dynamic challenges of digitisation (transformation process) but at the same time remain sufficiently scalable, so that in particular the topics of information and cyber security, digital sovereignty, technology and willingness to innovate, critical infrastructure and continuity management are addressed more closely in the administrative structure of Germany.

References

1. Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management.
2. Burkett, J. S. (2012). Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®. *Information Security Journal: A Global Perspective*, 21(1), 47-54.
3. German Federal Office for Information Security (2019) IT-Grundschutz Home. https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
4. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38, 97-102.
5. Shackelford, S. J., Russell, S., & Kuehn, A. (2016). Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors. *Chi. J. Int'l L.*, 17, 1.
6. Ausschuss für Bildung F. u. (2011). *Gefährdung und Verletzbarkeit* moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls. Berlin: Deutscher Bundestag, Drucksache 17/5672.
7. Mayring, P. (1983). *Qualitative Inhaltsanalyse. Grundlagen und Techniken*. Beltz Verlag, Weinheim 1983, 8. Auflage, Beltz, UTB, *Weinheim 2003*. Weinheim.
8. Mey, G. (2010). *Handbuch Qualitative Forschung in der Psychologie*. Wiesbaden: VS Verlag für Sozialwissenschaften Springer Fachmedien.
9. Dürig, M. (4/2018). Cybersicherheit in Kritischen Infrastrukturen. *Datenschutz und Datensicherheit (DuD)*.
10. Pfeiffer, S. (1/2019). Security-Management-as-a-Service. *Datenschutz und Datensicherheit (DuD)*.
11. Hackenjos, T. (5/2018). IT-Sicherheit- einrechtsfreier Raum. *Datenschutz und Datensicherheit (DuD)*.
12. Beyerer, J. (5/2018). *Karlsruher Thesen zur Digitalen Souveränität Europas*. *Datenschutz und Datensicherheit*.
13. Raabe, O. (11/2018). *Systematisierung des IT-Sicherheitsrechts*. *Computer und Recht*.
14. Dännert, S. (2018). *IT-Sicherheit in Kritischen Infrastrukturen- eine Fallstudie-basierte Analyse von Praxisbeispielen*. 85577 Neubiberg: Universität der Bundeswehr, Fakultät für Informatik.