Gunnar Auth und Tim Pidun (Hrsg.):
Fachtagung Rechts- und Verwaltungsinformatik (RVI 2023),
14 Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023

Federal Cybersecurity Architecture and Information Security Management

Adoption and Diffusion of the NIS-2 Requirements

Thomas Rehbohm [1] Frank Moses [2]

Abstract: Europe, the federal government, the federal states, municipalities, and their business enterprises are facing the challenges of a hybrid threat situation. At a time when information technology is growing faster than ever before, information cyber security and security management system (ISMS) assessment have become one of the most important aspects of most public sector organisations. The dependency on technology for almost every single process in public sector organisations has put ISMS at the top of the corporate agenda. For public organisations in particular, the NIS 2 Directive describes abstract requirements for the development of an ISMS. At the same time, minimum requirements should be defined that help municipal administration set up an information security management system quickly and easily. This paper summarizes the different requirements and generates a foundation for a rough procedural model, for implementing the upcoming requirements of the NIS 2 Directive quickly and easily in local governments. In particular, the current discussion focuses on securing ICT infrastructures and services of all providers of services of general interest. European and national regulations provide the framework for an appropriate response to this threat to the common good. The federal cybersecurity architecture of a member state such as Germany, presented here, must fit into the European context. Procedures for the implementation of information security management systems complement this theoretical model. This thesis presents a federal cybersecurity model.

Keywords: Security Architecture, Federal Government Institutions

1 Introduction

For a federal state in Germany, the respective member state and the European Union, the availability of important consumer goods and infrastructures is part of public services. The public administration is responsible as a guarantor at all levels of the protection of the

[1] Institute of Computer Science, University of Rostock Germany, Thomas.Rehbohm@uni-rostock.de

[2] Institute of Computer Science, University of Rostock Germany, Frank.Moses@uni-rostock.de

doi:10.18420/rvi2023-006

state, economy, and society [RiBM16, S.261], [WaWe20, S.710]. State institutions must act, since the Federal Republic of Germany and its states are obliged to place human needs, including economic ones, at the centre of their activities [Bund82, S.82–118].

The current threat situation leaves no room for discretion here, information security is endangered and thus higher than ever [Bund22a]. In particular, due to successful attacks on e.g., municipal IT infrastructures or on the IT systems of hospitals, Germany is also called upon to do more for the cooperation of all actors and for a common approach to strengthen resilience.

A functionally effective and federal cybersecurity architecture must be underpinned by the information security management systems of the respective actors. In this context, the strategy and motivation of the state, business and society as well as municipalities are fundamentally comparable, although it is recognized that commercial enterprises serve other stakeholders.

The architectural superstructure is to be produced in consultation with all the federal states and, at best, should be seamlessly embedded in European architecture. According to statements by the Federal Minister of the Interior on the expansion of the German BSI into a central office for cyber security matters, [Bund22b] a third security pillar is to be created along the lines of the Federal Criminal Police Office (BKA) and the Federal Office for the Protection of the Constitution (BfV). The transfer of competencies in the field of cyber security of the states, in favour of the federal government, may require adjustments but are not the focus of this work.

The research object of this thesis relates to an effective interaction of a federal cybersecurity architecture, which is substantiated with information security management systems - regardless of the framework included - according to the CISIS12 process model and adequately takes into account the requirements of the NIS 2 Directive [MoRe22] [Euro23].

In chapter 2 we give an overview of the state of the art. This is followed by chapter “3 Methodology" that describes the phases of the Design Science approach, which are progressed through step by step. Chapter "4 Federal Cybersecurity Architecture” describes the development of the cybersecurity architecture, considering the requirements of the NIS 2 Directive (chapter 5). These results were structured in a further step in order to develop and describe a rough process model based on them. The results will be used to realize an implementation in practice with the help of the CISIS12 process model (section 6). This process model has already been successfully tested in an artificial environment. Currently, the procedure model is being tested in a real environment with different test subjects. The section 7 briefly summarises the result.

The goal of our research is to identify the specifics of public sector organisations and develop an Cyber Security Architecture and ISMS Approach tailored to their demands. The current requirements of the NIS-2 Directive [Rich22] should be considered.

2 State of the art

Research contributions in the context of cyber and information security, combined with topics such as information security management systems, cybersecurity law and cybersecurity architectures, have continued to grow due to the current threat situation and topicality.

European contributions in the field of services of general interest are mainly concerned with internal market law, competition law and, in the context of structural and demographic change, with social, care and health systems. In principle, these are contributions that concern the common good but do not represent the services of general interest related to the ICT structures of a region. State interaction between actors in services of general interest is currently not a research focus; rather, contributions to cybersecurity law are in current discussions [KiBa20] or civil security [GuKW17] in the context of services of general interest. An in-depth literature review is part of the article "Security Management, Cyber Security and Services of General Interest: Empirical Study in German Municipalities" [RKCS22]. The following examples are extracted from this and are intended to illustrate the topic as examples.

The federal system of the United States is comparable to Germany. In "The Cybersecurity Policy Challenge – The Tyranny of Geography," Kamarck recommends that a seamless architecture of collaboration must emerge because, unlike governments, cybersecurity threats are borderless [Andr12].

At the European level, Krajweski's "Services of general interest beyond the single market" states that in the Treaty of Lisbon, the Member States (national, regional and local authorities) of the European Union, among others, have general responsibility for the "provision, commissioning and organisation" of services of general interest [Kraj15].

At the national level, the authors of "Cyber Security in Critical Infrastructures" state that the cooperative approach in the field of cyber security has proven its worth, especially because trusting cooperation between the state and business is a "shared mission" [DüFi18].

3 Methodology

This work is part of a research project aiming at methodical and technological support for cybersecurity architecture and information security management in public sector organisation units. The project follows the paradigm of design science research (DSR) [JoPe14]. DSR is a research paradigm aiming at problem-solving in organizational settings with a focus on developing valid and reliable knowledge for designing the required solutions. DSR research projects typically consist of several phases and require

the use of different research methods depending on the DSR phase and intended design solution.

This paper concerns the phase requirements definition and design and development of the design solution, i.e., the core artefact.

Table 1 provides an overview of the research activities performed in the different phases of the DSR process, the research methods used for these activities, the results achieved and the sections of this paper providing information about the results.

According to the DSR paradigm, the problem investigation must investigate two aspects: the knowledge base and the business relevance. The knowledge base consists in general of the published scientific work in the area under investigation. Using a literature analysis, we identified relevant existing work. The results presented in section 1 confirm that there is no tailored approach in science for a Cyber Security Architecture in the federal context. The business relevance has to show that the research challenge is not only relevant for a small number of organizations, i.e., an isolated "local" problem to solve but has substantial relevance in organizational practice and deserves research. In addition to previous studies confirming the general relevance of a Cyber Security Architecture implementation, a survey among Public Sector Organisations also confirms the existence of inhibiting factors. The **phase of requirements definition** in DSR addresses the initial definition of the core artefact that is supposed to address the **identified problems**, and the identification of requirements that the artifact must meet. The artefact in our context is a procedural approach tailored to the needs of Public Sector Organisations on how to introduce ISMS and the Cyber Security Architecture. The needs of Public Sector Organisations are expressed by the requirements which in turn are derived from the inhibiting factors in combination with identified success factors. **Design and development** of the artefact in DSR is an iterative process accompanied by demonstration or evaluation. As the artefact in its current form is documented in a handbook (already published [MoSa22]). **Demonstration** means exposing the first applicable version of the artefact to a real-world application case or experts from the field. Evaluation can use different strategies, like initial evaluation in a lab setting or evaluation in real-world cases. **As the artefact** already is used by many Public Sector Organisations, we chose a combination of real-world **evaluation** and evaluation based on the features of the artefact.

DSR Phase	Research activity	Result	Section / Literature
Problem Investigation	Literature analysis to determine the state of research	Inhibiting factors and critical success factors visible in the literature	section 1 [MoSK22a]
	A survey to determine business relevance	Inhibiting factors visible in the practice of Public Sector Organisations	section 2.2 [MoSK22b]
Define	Argumentative-deductive	Summary of inhibiting	section 4

Requirements	work to derive requirements from results of problem investigation	and success factors List of requirements	
Design and develop Artifact	Conceptual-deductive work to design procedural model based on requirements	ISM procedural model and handbook	summary of this paper section 4 [MoSa22]; [MoRe23]
Demonstrate	Application of Cyber Security Architecture	Not covered in this work	
Evaluate Artifact	Evaluation	Not covered in this work	

Table 1: Research activities performed in DSR phases and their results

First, we have primarily considered the requirements of the NIS-2 Directive in this document. At the same time, we have identified further important requirements through a literature review. We merged both lists of requirements to create an overarching list of requirements as a foundation for the development of a rough procedural model.

4 Federal Cyber Security Architecture

Cyber Security architectures should be an elementary component of digital services of general interest in Germany's federal system. [Scha18] Essential actors of a regional structure must be actively connected in such a way that joint interaction can take place before, during and after cybersecurity events. The architectures, which are as harmonious as possible between the federal states, together with the federal government, represent the level of overall security that meets the requirements of European regulation. Initially, the core processes and support processes as well as the processes for the strategy of an enterprise architecture are modelled in the architecture. The inter-organizational process design of the cybersecurity organization is documented as an enterprise architecture that is to be further developed into a reference architecture. The modelling of the reference architecture was done in the modelling language ArchiMate and is shown as an example in Figure 1 on the top. In addition to research, enterprise architecture management has also evolved to provide practical support for decision-support functions in organizations such as administration [SiFS14].

The research presented here aims to determine the interlocking of a federal architecture with the information security management systems of the systemically important actors. Within the framework of a study and expert interviews, various requirements and goals for a federal Cyber Security Architecture were derived [ReKa22], [RKCS22], [RSCK22] and [ReSK00].

The foundation of such an architecture is formed by the support processes, namely **legislative processes**. Furthermore, **communication and cooperation**.

The pillars of the actual Cyber Security Architecture are built on this foundation.

- Compliance
- Risk management
- Operation
- Control and improvement
- Safety standards

On top of these supporting pillars lies the level of strategy and motivation as an umbrella.

Legislative processes: This is an essential support process that includes the obligation of the federal states to initiate legislation and regulations in line with external and internal requirements and to adapt them to the changed European regulations.

Communication and cooperation include all necessary actors and tasks to detect and defend against cybersecurity threats.

Within the framework of the core processes (pillars of the architecture), the following tasks are focused on:

Compliance: Initial and recurring identification of essential legal frameworks.

Risk Management: Monitoring the change in threats to the federal infrastructure and related threats to it and related processes.

Operation: All tasks that guarantee the operation of the cybersecurity architecture.

Control and improvement: Steering committee for assessing resilience and deriving concrete measures to maintain or improve it.

Security standards: All tools, measures and procedures that promote operations on the one hand and the resilience of the cybersecurity architecture on the other, especially in information security.

This cybersecurity architecture aims to achieve the following objectives: legal certainty, applicability, resilience, sustainability, and cooperation. **Strategy and motivation are the** umbrella process that is mapped in the architecture and visualizes the expectations of the stakeholders.

In addition to these two dimensions of "**strategy, core and support processes" and** "**goals**", the cybersecurity architecture consists of another dimension. These are processes that can be individually designed by the users to the respective context. The figure below summarizes these three dimensions (Figure 1**)**

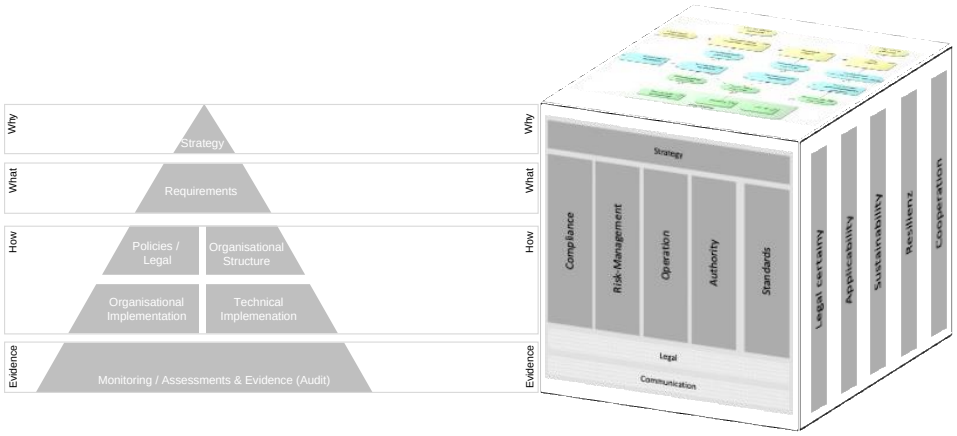

Figure 1: Cybersecurity Cube (Architecture, Goals, and Processes)

5 NIS 2 Directive

The Network and Information Systems Directive 2 (NIS-2) [Weis23] is a European directive that aims to improve cybersecurity in critical infrastructures and digital services. It significantly expands the scope and obligations of the previous Directive and thus provides for various measures to achieve the objective of improved resilience, including:

- **Mandatory security requirements**: Operators of critical infrastructure and digital services must implement appropriate safeguards to identify and prevent threats.
- **Security incident reporting**: Operators must report security incidents to national authorities and share information about these incidents to improve response capability.
- **Establishment of CSIRTs**: National authorities must establish Computer Security Incident Response Teams (CSIRTs) to respond to security incidents.
- **Regular security audits**: Operators must conduct regular security audits and review their security measures to ensure they are adequate and in line with current threats.
- **Cooperation between Member States**: Member States need to work together and share information to join Cybersecurity Cube (Architecture, Goals, and Processes) to combat threats and improve cybersecurity in Europe.

These measures are intended to ensure that critical infrastructures and digital services in Europe, including Germany, are safe and secure, and that they can respond to threats and prevent attacks. In practice, the development and sustainable establishment of an information security management system (ISMS) form an essential foundation for the implementation of the NIS 2 Directive, as an ISMS helps to ensure the security of critical infrastructures and digital services and to respond quickly and effectively to

threats.[EcKo23] In Art. 21 of the NIS 2 Directive, four **core requirements** are formulated that must be met by an ISMS [Weis23]. These include:

- **Policies**: Risk & Information Security Policies
- **Incident Management**: Prevention, detection, and management of cyber incidents
- **Business Continuity**: Business Continuity Management, Crisis Management
- **Supply Chain Management**: Security in the supply chain — up to secure development at suppliers
- **Procurement**: Security in the procurement of IT and network systems
- **Effectiveness**: Requirements for measuring cyber and risk measures
- **Training**: and Cyber Security Hygiene
- **Cryptography**: Specifications for cryptography and, where possible, encryption
- **Personal**: Human Resources Security
- **Physical access control**
- **Asset Management** (ISMS)
- **Authentication**: Use of multi-factor authentication (MFA) and single sign-on (SSO)
- **Communication**: Use of secure voice, video, and text communication
- **Emergency communication**: Use of secure emergency communication systems

At this point, the cyber security architecture described above provides a frame of **reference**. First and foremost, a **strategy** must be formulated by the deploying organisation to define the why in the implementation of the cyber security architecture. This is followed by the definition of **requirements** for the respective context. The organizational and **technical implementation** of the requirements is coordinated by an appropriate **organizational structure** and flanked by appropriate **guidelines**. Corresponding evidence must be generated, for example, by audits, which can then also be used as **proof of guarantee** against third parties.

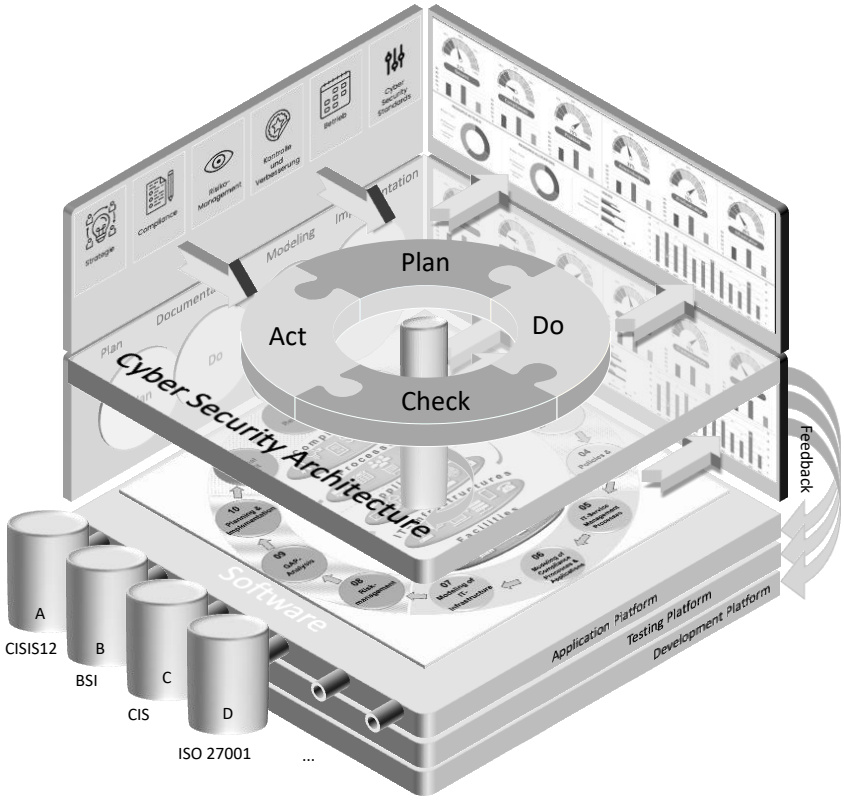

Figure 2: Cyber Security Architecture with ISMS

The elements of the cybersecurity strategy are complemented by the cybersecurity strategy (Figure 2**)**. After the theoretical derivation, strategy, requirements, and implementation measures must now be transferred to a practicable procedural model. First and foremost, the requirements of the core processes of the cybersecurity architecture act on an axis of rotation, which in turn drives the development and establishment of an ISMS. With the help of the Deming Circle, individual adaptations from the cybersecurity architecture can be transferred to the ISMS. From the ISMS, aggregated results are fed back into the control centre of the higher-level cybersecurity architecture, which allows the legally required supervisory management to be fulfilled. The user can decide for himself which standard (BSI baseline protection, ISO/IEC 27001, or others) should be used to set up and establish the ISMS.

6 CISIS12

Public organisations in particular often lack the necessary resources and expertise to set up an ISMS with which the measures formulated in the NIS 2 Directive can be implemented [MoSK22c]. Here, the CISIS12 (Compliance and Information Security in 12 Steps) process model [MoRe23] offers a quick and easy introduction to the topic of ISMS for public organizations [MoSa22].

Step 1 Guideline: The focus of the first step is the creation of a guideline on information security as one of the reference documents of the CISIS12 standard and an essential element of an ISMS.[MoSK22c] **Step 2 Raising awareness among employees**: In many projects, the consideration of employees is only at the end of the project [TFSG18]. However, it is precisely the issue of cyber security that primarily affects employees and managers. As part of step 2, a process must be established based on an appropriate concept to ensure training, sensitisation, and information for employees. However, it is important that after employees have been sensitized for the first time, sustainability is ensured by the training concept in a target group-specific manner. **Step 3 Information security team**: The roles necessary for the development of the ISMS are fixed here in writing, tasks, rights and obligations are defined and an ISMS team is formed. Depending on the size of the organization, it is necessary to determine with which roles the upcoming ISMS project is to be carried out and which employees have roles in the core team and which employees have roles in the extended security team. Regardless of this organizational structure, a member of the organizational leadership must be integrated into the extended team in any case [ChMC16]. **Step 4 IT documentation structure**: The PDCA cycle immanent in a management system focuses on the "P for plan". No successful project, without a good plan. Against this background, step 4 of the CISIS12 process model focuses on the creation and updating of a documentation structure suitable for the ISMS [SuOY22]. Documentation that is intended to support the organization in the operation of the ISMS on the one hand, but also serves as proof of certification on the other, must meet the requirements of structure, clarity, completeness, comprehensibility, correctness, traceability, objectivity, integrity, and authenticity. The CISIS12 standard lists the 16 mandatory documents (e.g., guidelines, training and awareness-raising concept, operating manual and network plan to a management report including implementation and risk treatment plan and emergency manual). In addition to these certification-relevant reference documents, further documents are inevitably created when the 12 steps are completed, e.g. work instructions, process descriptions or concepts. Almost all documentation must be made known to the employees and therefore controlled. **Step 5 IT service management**: One of the main differences to other ISMS process models is the implementation of IT service management in the CISIS12 process model. The implementation of clearly defined and described IT service management processes is a key success factor for increasing information security and .dem maturity of the ISMS [Awan17]. In step 5, the three essential IT service management processes (maintenance, malfunction and change processes) are to be set up in an organization-specific manner or

the processes that already exist in reality are to be integrated into the ISMS and further developed. **Step 6 Compliance, Processes and Applications**: CISIS12 has taken up the requirements from practice, namely, to integrate the legal requirements and contractual obligations (compliance) as well as the process view into the management system and includes five levels of consideration, namely the compliance and process layer as well as the application and infrastructure and building level. Thus, CISIS12 offers a view that corresponds to that of the management level, namely "Which legal requirements and compliance requirements must the management level meet and how can these be implemented in practice (corporate governance)?". Thus, the CISIS12 process model makes it easier for the management level to act and delegate the necessary tasks to set up and establish an ISMS while at the same time meeting the legal requirements and minimizing the liability risks of the management level. This means that in **step 6**, the business processes that are essential for the organization are identified and evaluated concerning the protection requirements of confidentiality, integrity, and availability. This can be done with the help of tools, as can the assignment of modules and measures. **Step 7** IT infrastructure: The recording of IT infrastructure objects (e.g. servers, clients, active network components, etc.) is derived from the business processes identified in step 6 and the applications necessary for these business processes and forms an important pillar of the ISMS [ChKP22]. Thus, a simplification for the user also occurs here. In this way, attention can be drawn to the implementation of the module and measure assignment. **Step 8 Risk management**: Risk management is a major innovation in the CISIS12 process model [KiCK22]. The geopolitical events of the past few months have shown that the development of an information security management system is no longer a hygiene factor (hygiene factor = works without it, but a little worse). No, an ISMS is now a "must-have" (state of the art) for all organizations and a risk management system established in it is an important tool for learning from the past and being able to better assess future events. **Step 9 Target/actual comparison**: In step 9, the measures from the CISIS12 building block catalogue modelled in steps 6 and 7 are evaluated concerning the degree of implementation. This evaluation process takes place within the framework of a group dynamic process and represents a self-evaluation. This process may be supported by external third parties. **Step 10 Implementation**: The degree of implementation of the individual measures determined in Step 9 can be transferred to an implementation plan in Step 10 with the help of tools, if necessary. Individual measures can be prioritized, their financial and personnel expenses can be recorded, and the roles of the initiator and the implementer can be defined with the help of tools. No system is perfect, and more is always possible. This also applies to the ISMS built with CISIS12. The maturity level of a management system with CISIS12 only develops with several runs. The initial audit is therefore referred to as a system audit, whereby the certification audit focuses on the documentation and implementation of the plan documents (lived security process). The surveillance audit then examines how the ISMS has developed further and how this further development affects the maturity level. **Step 11 Internal Audit**: In step 11, CISIS12 requires the organization to create an appropriate audit program. This audit program

should then include the respective certification as well as internal audits. With the help of internal audits, the organization itself should be able to examine its own ISMS for weaknesses and improve it accordingly [Pohl19]. **Step 12 Revision**: CISIS12 steps 1 to 11 must be completed regularly (e.g. annually). However, changes and additions can also be introduced into the management system at any time. Step 12 summarizes the results of the final PDCA phase and ends with the preparation of a management report. Step 12 summarizes the results of the final PDCA phase and ends with the preparation of a management report. At the same time, the management report is one of the certification-relevant reference documents. As soon as the management level has approved the management report including its assets, the next PDCA phase can begin and the continuous improvement process can be initiated [PrSu22]. The entire process is supported by the CISIS12 circuit – possibly tool-based.

7 Summary, Conclusions and Outlook

The NIS 2 Directive requires in Art. 21 fourteen measures to be implemented by federal states. The developed cybersecurity architecture forms a good procedural model for identifying, planning, implementing and sustainably establishing and controlling these measures and associated requirements. An essential tool here is the selection of a suitable process model for the further implementation of an information security management system as the basis of a higher-level cybersecurity architecture. The presented cybersecurity architecture can be used can be underpinned by the CISIS12 process model. The implementation of CISIS12 is open. An ISMS can be set up with the native CISIS12 catalogue. However, it is also possible to use other module measure catalogues with the process model, e.g., "BSI-IT-Grundschutz", "BSI-Kommunalprofil" or ISO/IEC 27001, CIS-Controls, or other proprietary measures. In particular, the aspects of the NIS 2 guideline such as guidelines, awareness and training measures for employees, incident management, business continuity management and implementation of technical and organizational measures can be implemented in a target group-adapted manner with the help of the CISIS12 process model. The result is an overall cybersecurity architecture that can meet the requirements of the NIS 2 Directive. It does not matter whether users choose a top-down approach or a bottom-up approach. Due to the interlocking of the two architectures, each approach can be started independently of the other and the necessary information can be exchanged via interfaces (Figure 1**)**.

One limitation of the present work is that the presented theoretical cybersecurity architecture has not yet been evaluated practically. Plans are currently underway to verify the architecture in conjunction with the establishment of an ISMS in a municipal organization. The logical final step is the evaluation of the overall architecture in the country context. For this purpose, the overall architecture is to be presented within the framework of the working group on the cyber security of the federal states. Depending on the evaluation results, the architecture will be further developed.

References

[Andr12] Andreasson, K. J. (Hrsg.): Cybersecurity: public sector threats and responses, Public administration and public policy. Boca Raton, FL : CRC Press, 2012 — ISBN 978-1-4398-4663-6

[Awan17] Awan, Jawad Husaain: Security strategies to overcome cyber measures, factors and barriers. In: Engineering Science and Technology International Research Journal Bd. Vol.1, No. 1 (2017)

[Bund22a] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2022 (2022)

[Bund22b] Bundesministerium des Innern und für Heimat: Bundesinnenministerin stellt Cybersicherheitsagenda vor. URL https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2022/07/cybersicherheitsagenda.html. — Bundesministerium des Innern und für Heimat

[Bund82] Bundesverfassungsgericht: Entscheidungen der amtlichen Sammlung - 2 BvR 1187/80. Bd. 61, 1982

[ChKP22] CHODAKOWSKA, ANETA; KAŃDUŁA, SŁAWOMIRA; PRZYBYLSKA, JOANNA: Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done. In: Lex Localis - Journal of Local Self-Government Bd. Vol. 20, No. 1 (2022)

[ChMC16] Choejey, Pema ; Murray, David ; Che Fung, Chun: Exploring Critical Success Factors for Cybersecurity in Bhutan's Government Organizations. In: Computer Science & Information Technology (CS & IT) : Academy & Industry Research Collaboration Center (AIRCC), 2016 — ISBN 978-1-921987-60-1, S. 49–61

[DüFi18] Dürig, Markus ; Fischer, Matthias: Cybersicherheit in Kritischen Infrastrukturen: Europäische und deutsche Regulierung — ein Überblick. In: Datenschutz und Datensicherheit - DuD Bd. 42 (2018), S. 209–213

[EcKo23] Eckhardt, Philipp ; Kotovskaia, Anastasia: The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. In: International Cybersecurity Law Review Bd. 4 (2023), Nr. 2, S. 147–164

[Euro23] Europäisches Parlaments und Rat: Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie), 2023

[GuKW17] Gusy, C. ; Kugelmann, D. ; Würtenberger, T. (Hrsg.): Rechtshandbuch Zivile Sicherheit. Berlin Heidelberg : Springer, 2017 — ISBN 978-3-662-53288-1

[JoPe14] Johannesson, Paul ; Perjons, Erik: An Introduction to Design Science. Cham : Springer International Publishing, 2014 — ISBN 978-3-319-10631-1

[KiBa20] Kipker, D.-K. ; Barudi, M. (Hrsg.): Cybersecurity. 1. Auflage. München : C.H. Beck, 2020 — ISBN 978-3-406-73011-5

[KiCK22] Kitsios, Fotis ; Chatzidimitriou, Elpiniki ; Kamariotou, Maria: Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security

Management Systems: A Case Study in IT Consulting Industry. In: Sustainability Bd. 14, Multidisciplinary Digital Publishing Institute (2022), Nr. 3, S. 1269

[Kraj15] Krajewski, M. (Hrsg.): Services of general interest beyond the single market: external and international law dimensions, Legal issues of services of general interest. The Hague : T.M.C. Asser Press, 2015 — ISBN 978-94-6265-062-6

[MoRe22] Moses, Frank ; Rehbohm, Thomas: CISIS12. In: , CISIS12. (2022), Nr. 1, S. 11

[MoRe23] Moses, Frank ; Rehbohm, Thomas: CISIS12 für kleine und mittelständische Organisationen IN ZWÖLF SCHRITTEN ZUM RECHTSKONFORMEN ISMS (2023), Nr. 4, S. 14–19

[MoSa22] Moses, Frank ; Sandkuhl, Kurt: Mit CISIS12 ein ISMS aufbauen. In: Datenschutz und Datensicherheit - DuD Bd. 46 (2022), Nr. 10, S. 654–659

[MoSK22a] Moses, Frank ; Sandkuhl, Kurt ; Kemmerich, Thomas: Information security management in German local government. In: , 2022, S. 183–189

[MoSK22b] Moses, Frank ; Sandkuhl, Kurt ; Kemmerich, Thomas: Empirical Study on the State of Practice of Information Securty Maturity Management in Local Government. In: Zimmermann, A. (Hrsg.): Human Centred Intelligent Systems 2022 - Proceeding of the 15th International Conference on Human Centred Intelligent Systems (KES-HCIS-22). Smart Innovation, Systems and Technologies. : Springer. Accepted for publication. To appear June 2022., 2022

[MoSK22c] Moses, Frank ; Sandkuhl, Kurt ; Kemmerich, Thomas: Empirical Study on the State of Practice of Information Security Management in Local Government. In: Zimmermann, A. ; Howlett, R. J. ; Jain, L. C. (Hrsg.): Human Centred Intelligent Systems, Smart Innovation, Systems and Technologies. Singapore : Springer Nature, 2022 — ISBN 978-981-19345-5-1, S. 13–25

[Pohl19] Pohlmann, Norbert: Cyber-Sicherheit: das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung. Wiesbaden : Springer Vieweg, 2019 — ISBN 978-3-658-25397-4

[PrSu22] Preis, Benjamin ; Susskind, Lawrence: Municipal Cybersecurity: More Work Needs to be Done. In: Urban Affairs Review Bd. 58, SAGE Publications Inc (2022), Nr. 2, S. 614–629

[ReKa22] Rehbohm, Thomas ; Kalmbach, Peter: MMR-Aktuell 2021, 438461 - beck-online, Grundforderungen von Informations- und Cybersicherheit in Ländern. URL https://beck-online.beck.de/?vpath=bibdata/zeits/MMRAktuell/2021/438461.htm. - abgerufen am 2022-09-08

[ReSK00] Rehbohm, Thomas ; Sandkuhl, Kurt ; Kemmerich, Thomas: On Challenges of Cyber and Information Security Management in Federal Structures - The Example of German Public Administration. In: , S. 13

[RiBM16] Riek, Markus ; Bohme, Rainer ; Moore, Tyler: Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. In: IEEE Transactions on Dependable and Secure Computing Bd. 13 (2016), Nr. 2, S. 261–273

[Rich22] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie). Bd. 333, 2022

[RKCS22] Rehbohm, Thomas ; Kemmerich, Robin ; Cap, Clemens H. ; Sandkuhl, Kurt: Sicherheitsmanagement, Cybersicherheit und Daseinsvorsorge: Empirische Studie in deutschen Kommunen. In: Datenschutz und Datensicherheit - DuD Bd. 46 (2022), Nr. 7, S. 448–454

[RSCK22] Rehbohm, Thomas ; Sandkuhl, Kurt ; Cap, Clemens H. ; Kemmerich, Thomas: Integrated Security Management of Public and Private Sector for Critical Infrastructures – Problem Investigation. In: Abramowicz, W. ; Auer, S. ; Stróżyna, M. (Hrsg.): Business Information Systems Workshops, Lecture Notes in Business Information Processing. Cham : Springer International Publishing, 2022 — ISBN 978-3-031-04216-4, S. 291–303

[Scha18] Schallbruch, Martin: Schwacher Staat im Netz: wie die Digitalisierung den Staat in Frage stellt. Wiesbaden : Springer, 2018 — ISBN 978-3-658-19946-3

[SiFS14] Simon, Daniel ; Fischbach, Kai ; Schoder, Detlef: Enterprise architecture management and its role in corporate strategic management. In: Information Systems and e-Business Management Bd. 12 (2014), Nr. 1, S. 5–42

[SuOY22] Susukailo, Vitalii ; Opirsky, Ivan ; Yaremko, Oleh: Methodology of ISMS Establishment Against Modern Cybersecurity Threats. In: Klymash, M. ; Beshley, M. ; Luntovskyy, A. (Hrsg.): Future Intent-Based Networking, Lecture Notes in Electrical Engineering. Cham : Springer International Publishing, 2022 — ISBN 978-3-030-92435-5, S. 257–271

[TFSG18] Tatiara, R. ; Fajar, A. N. ; Siregar, B. ; Gunawan, W.: Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001. In: Journal of Physics: Conference Series Bd. 978, IOP Publishing (2018), Nr. 1, S. 012039

[WaWe20] Watson, Richard T. ; Webster, Jane: Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0. In: Journal of Decision Systems Bd. 29, Taylor & Francis (2020), Nr. 3, S. 129–147

[Weis23] Weissmann, Paul: Die neue EU NIS 2 Direktive für Cyber Security in KRITIS. URL https://www.openkritis.de/it-sicherheitsgesetz/eu-nis-2-direktive-kritis.html. - abgerufen am 2023-05-09