Universität Rostock

Traditio et Innovatio

WIRTSCHAFTSINFORMATIK
UNIVERSITÄT ROSTOCK

Procedural Model for the Adoption of ISMS in Small Public Sector Organisations

DISSERTATION

to obtain the academic degree of

DOKTOR-INGENIEUR (DR.-ING.)

of the Faculty of Computer Science and Electrical Engineering

at the University of Rostock

submitted by

Frank Moses

Master of Science

born on 15.06.1968 in Brebach, Germany

Rostock, 29.07.2024

https://doi.org/10.18453/rosdok_id00004775

Reviewers:

Prof. Dr. Kurt Sandkuhl, University of Rostock, Institute of Computer Science

Prof. Dr. Michael Fellmann, University of Rostock, Institute of Computer Science

Prof. Dr. em. Thomas Kemmerich, NTNU Trondheim, Norway

Date of defense:

21.01.2025

Abstract

Threats from cyberspace are increasing more and more. These threats affect not only companies but also administrations. The automated processing of information and data now plays a crucial role in fulfilling tasks in local governments. The complexity of information technology, the increasing degree of networking, and the dependence on IT-supported processes require that the security of information technology has an ever-higher priority. Due to the increased dependence on modern ICT, the risk of information infrastructures being impaired by deliberate attacks from within and outside, negligent actions, ignorance, or technical failure has increased significantly, both qualitatively and quantitatively. Small local governments face the same risks as large organisations but are more vulnerable at any given time due to reduced resources.

Previous research work focuses on the framework conditions of the corporate environment. These frameworks cannot transfer to administrations without revision, and thus, provided concepts, strategies, or even recommendations for action were not suitable to the requirements of governments.

This thesis develops, describes and evaluates a procedural model with a supporting software component for developing and establishing an information security management system for the target group of small local governments.

In this way, the framework conditions, designs and effects of implementing the process model can be shown and examined both in science and practice. The procedural model was tested on 24 test subjects under natural conditions and extended to other clients over time.

The overall development of the concept was implemented with the help of data mining tools to react proactively to changes in the environment and threat scenarios from cyberspace and thus ensure the organisation's resilience in the long term.

The thesis uses a design science approach as an overarching research paradigm. In summary, implications, limitations and possibilities for future research are derived.

Keywords: Information Security, Cybersecurity, ISMS, Local Government, Prediction

Kurzfassung

Bedrohungen aus dem Cyberraum nehmen mehr und mehr zu. Davon sind nicht nur Unternehmen betroffen, sondern auch Verwaltungen. Die automatisierte Verarbeitung von Informationen und Daten spielt mittlerweile eine Schlüsselrolle bei der Aufgabenerfüllung in Kommunalverwaltungen. Die Komplexität der Informationstechnik, der zunehmende Grad der Vernetzung und die Abhängigkeit von IT-gestützten Verfahren erfordern es, dass die Sicherheit der Informationstechnik einen immer höheren Stellenwert einnimmt. Durch die verstärkte Abhängigkeit von moderner IKT hat sich das Risiko der Beeinträchtigung von Informationsinfrastrukturen durch vorsätzliche Angriffe von innen und außen, durch fahrlässiges Handeln, Unkenntnis oder technisches Versagen sowohl qualitativ als auch quantitativ deutlich erhöht. Insbesondere kleine Kommunalverwaltungen sind mit den gleichen Risiken konfrontiert wie große Organisationen, sind aber aufgrund der geringeren Ressourcen zu jedem Zeitpunkt gefährdeter.

Bisherige Forschungsarbeiten waren an schwer übertragbare Rahmenbedingungen aus dem Unternehmensumfeld orientiert und lieferten so Konzepte, Strategien oder auch Handlungsempfehlungen, die nicht auf die Anforderungen der Kommunalverwaltung angepasst waren.

Die vorliegende Arbeit entwickelt, beschreibt und evaluiert ein prozedurales Vorgehensmodell mit einer unterstützenden Softwarekomponente zum Aufbau und Etablierung eines Informationssicherheitsmanagementsystems für die Zielgruppe kleine Kommunalverwaltungen.

Damit können sowohl in Wissenschaft als auch Praxis die Rahmenbedingungen, Ausgestaltungen als auch Auswirkungen der Implementierung des Vorgehensmodells gezeigt und untersucht werden. Das Verfahren wurde bei 24 Probanden unter realen Bedingungen getestet und im weiteren Zeitverlauf auf weitere Mandanten ausgedehnt.

Die Weiterentwicklung des Gesamtkonzepts wurde mit Hilfe von Data-Mining-Werkzeugen umgesetzt, um so auf Veränderung der Umwelt und Bedrohungsszenarien aus dem Cyberraum proaktiv reagieren zu können und somit die Resilienz der Organisation nachhaltig sicherzustellen.

Die Arbeit setzt als übergeordnetes Forschungsparadigma einen Design Science Ansatz ein. Zusammenfassend werden Implikationen, Limitationen und Möglichkeiten für zukünftige Forschungen abgeleitet.

Stichworte: Informationssicherheit, Cybersicherheit, ISMS, Kommunalverwaltung, Vorhersagen

Acknowledgements

The entire research work, the preparation of publications, the development of the process model and the supporting software up to the creation of this dissertation would not have been possible without the support of various colleagues, friends and family.

A significant contribution to this dissertation was made by Dr. Birger Lantow, who provided advice and support in literature research and other things at the beginning of my research work. I often think of him and wish him all the best for his return to life!

I would like to express my special thanks to Prof. Dr. Kurt Sandkuhl, who offered me excellent research and working environment at his chair and contributed significantly to the successful completion of the thesis through his continuous, personal and committed supervision. His advice has been instrumental in developing me as a researcher.

I also thank Prof. Dr. Thomas Kemmerich and Prof. Dr. Michael Fellmannfor taking over the second corrector. Their suggestions on the overall approach of the thesis and many discussions regarding individual contributions were precious to me.

While preparing the thesis, I received valuable suggestions from various colleagues. In this context, I would like to mention Ms. Trish Quinn and Ms. Sandra Wagner, who supported me in the intricacies of the English language. In addition, the research assistants Niclas Carlsson, Sahib Niyazov and Jonathan Zelfel provided support in the context of literature research and preliminary analyses.

Martin Kuschke, who played a leading role in developing the application system and operating the application platform, is also not to be forgotten.

Special thanks goes to Ralf Turban, who supported many field experiments with words and deeds from the beginning.

I would also like to thank Andreas Storb for a quarter of a century of friendship and his support during this research project and in many private matters.

However, my most tremendous thanks go to my wife, who fought the battle with the error devil many times. I even thank her for her infinite patience during my research trip. But I also thank her for the strength she gave me in the difficult hours. Thank You! This work is therefore dedicated to her.

Danksagung

Die gesamte Forschungsarbeit, die Erstellung von Publikationen, Entwicklung des Vorgehensmodells als auch der stützenden Software bis hin zur Erstellung dieser Dissertation wäre nicht ohne die Unterstützung verschiedener Kollegen, Freunde und Familie möglich gewesen.

Einen wesentlichen Beitrag hat Dr. Birger Lantow zu dieser Dissertation gelegt, der zu Beginn meiner Forschungsarbeit bei Literaturrecherchen und weiteren Dingen mit Rat und Tat zu Seite gestanden hat. Ich denke sehr oft an ihn und wünsche ihm für die Rückkehr ins Leben alles nur erdenklich Gute!

Meinen besonderen Dank möchte ich Prof. Dr. Kurt Sandkuhl ausdrücken, der mir nicht nur ein ausgezeichnetes Forschungs- und Arbeitsumfeld an seinem Lehrstuhl geboten hat, sondern durch seine kontinuierliche, persönliche und engagierte Betreuung maßgeblich zum erfolgreichen Abschluss der Arbeit beigetragen hat. Sein Rat hat wesentlich dazu beigetragen mich als Forscher zu entwickeln.

Ebenso danke ich Prof. Dr. Thomas Kemmerich und Prof. Dr. Fellmann für die Übernahme des Koreferats. Ihre Anregungen zum Gesamtansatz der Arbeit als auch viele Diskussionen bezüglich einzelner Beiträge waren für mich sehr wertvoll.

Während der Erstellung der Arbeit habe ich von verschiedenen Kollegen wertvolle Anregungen erhalten. In diesem Zusammenhang möchte ich insbesondere Frau Trish Quinn als auch Frau Sandra Wagner erwähnen, die mich bei den Feinheiten der englischen Sprache unterstützt haben. Ferner waren die wissenschaftlichen Hilfskräfte Niclas Carlsson, Sahib Niyazov und Jonathan Zelfel im Rahmen von Literaturrecherchen und -Voranalysen unterstützend tätig.

Nicht zu vergessen ist Martin Kuschke, der bei der Entwicklung des Anwendungssystems und dem Betrieb der Anwendungsplattform federführend unterstützt hat.

Besonderer Dank geht an Ralf Turban, der viele Feldexperimente der ersten Stunde mit Rat und Tat unterstützt hat.

Ebenso möchte ich Andreas Storb danken, nicht nur für ein viertel Jahrhundert Freundschaft, sondern auch für seine Unterstützung während dieses Forschungsprojektes und auch in vielen privaten Dingen.

Mein aller größter Dank geht jedoch an meine Frau, die viele Male den Kampf mit dem Fehlerteufel gefochten hat. Noch viel mehr danke ich ihr für die unendliche Geduld, die sie während meiner Forschungsreise aufgebracht hat. Aber auch danke ich ihr für die Kraft, die sie mir in den schweren Stunden gegeben hat. Danke! Ihr sei daher diese Arbeit gewidmet.

Index

List of Figures

List of Tables

Abbreviations

AWC	Ability-Willingness-Consequences
BCM	Business Continuity Management
BI	Business Intelligence
BSI	Bundesamt für Sicherheit in der Informationstechnologie (engl. Federal Office for Information Security)
CIA	Confidentiality, Integrity, and Availability
CISO	Chief Information Security Officer
DSGVO	Datenschutzgrundverordnung (engl. General Data Protection)
DSR	Design Science Research
DSRP	Design Science Research Process
GDPR	General Data Protection Regulation
GRC	Governance Risk Compliance
ISM	Information Security Management
ISMS	Information Security Management System
ISO	Information Security Officer
ITIL	IT Infrastructure Library
ITSM	IT Service Management
KBA	Kraftfahrtbundesamt (engl. Federal Motor Transport Authority)
KPI	Key Performance Indicator
LDK	Leistungsdeterminantenkonzept (engl. AWC)
NIS2	Network and Information Systems Directive #2
OZG	Onlinezugangsgesetz (engl. Online Access Act)
PM	Project Management
SoA	Statement of Applicability
SPSO	Small Public Sector Organisation

PART A – INTRODUCTION AND FOUNDATIONS

The problem is not the problem.

The problem is your attitude about the problem.

Jack Sparrow

Part A of this dissertation primarily describes the problem and the motivation for preparing the present thesis. This is followed by a description of the research methods and which of them are used in the work. It is also necessary to explain various terms and to create a thematic delimitation with the help of the essential chapters.

1 Introduction

1.1 Problem Definition and Motivation

A functioning state is characterized by an efficient administration (Hopp, 2020, p. 19). The public sector needs to implement more and more modern solutions to maintain the performance and efficiency of its services (Wind, 2006, p. 7).

One focus here is on the digitization of administration (Schwab et al., 2020, p. 438). The digitization of business processes in public administration is also associated with risks (Schünemann, 2020, p. 200). The German Federal Office for Information Security (BSI) confirms this in its 2020 situation report, stating that the number of cyber-attacks on public administration increased, and a "new" quality of attacks has also been reported. Furthermore, the BSI emphasizes that the digitalization push triggered by the COVID-19 pandemic in state and local governments offers an increased attack surface (BSI, 2020, pp. 10, 33).

This situation has worsened since the war of aggression against Ukraine (BSI, 2022, p. 45). Against this background, it becomes clear that information security is indispensable today (Scholl, 2018, p. 162). As part of organizational management, it must be aligned to optimally support the business goals (Scholl, 2018, p. 161). This applies not only to companies but also to public administrations.

Especially in times of increasing cyber threats, a structured information security management system (ISMS) offers the optimal basis for efficiently and effectively supporting a holistic security strategy. Based on such a strategy, a Governance Risk Compliance System (GRC) can be set up to maintain, among other things, compliance with legal requirements such as the protection of personal data and the security of information (Bostelmann, 2021, p. 187).

To meet these requirements, an ISMS can support an organization through a cycle of planning, implementation, and evaluation (Schläger and Thode, 2022, p. 575). To this end, the international standard ISO 27001 has primarily established itself in business practice (Schläger and Thode, 2022, p. 581).

For the public sector, the German Federal Office for Information Security (BSI) provides a comprehensive catalogue of measures and various implementation recommendations – the so-called IT baseline protection – to support public organisations in setting up and establishing an ISMS (Frankenstein, 2023).

At the same time, at its 10th meeting in March 2013, the Federal Government's IT Planning Council committed the states to establish an ISMS in the federal states with guidelines for information security (Schulz, 2015, p. 471). Despite these efforts and existing funding programs for public organizations, there are still no significant successes in establishing ISMS in the German local government (BSI, 2022, p. 103). This may be due, on the one hand, to the tight municipal budgets or the typical administrative action of "reaction instead of action" or, on the other hand, to the lack of a suitable procedural model for the domain of local government.

There seems to be little truth in the latter point because the models for introducing an ISMS established in companies cannot be adopted in small local governments without revision (Hopp, 2020, p. 17).

Small public sector organisations (SPSO) are organisations with only a few employees (Schmid, 2019, p. 102), (Al Yami et al., 2021). Furthermore, information or cyber security is not the core task in such organisations due to the lack of resources and expertise (Rawindaran et al., 2023, p. 1). Nevertheless, they have to fulfil many tasks while taking cyber threats into account (Fujs and Bernik, 2024).

Against this background, the idea arose to develop a process model for introducing an ISMS adapted to the particular requirements of small and medium-sized administrations. The system's openness is considered to take any direction of development as requirements grow.

The present dissertation aims at both academia and practice. For this reason, it deals with both the need for theoretical and practical knowledge. At the same time, it addresses the subsequent research gaps and pursues the goal of generating new findings for both target areas by answering them:

1. **Research Gap:**
   On the one hand, companies have established process models for setting up an information security management system (Schläger and Thode, 2022, p. 584ff). On the other hand, the BSI provides a comprehensive work of measures in the form of IT-Grundschutz and a detailed framework for the federal and state administrations in the form of IT-Grundschutz Compendium (Frankenstein, 2023, p. 415).
   However, no process model is tailored to the particular requirements of small to medium-sized organizations in the municipal administration sector (Hopp, 2020, p. 17), (Markus and Meuche, 2022, p. 209). Therefore, these requirements from the target domain must first and foremost be determined and analyzed. These insights can be used to understand the target domain and its processes and challenges.
2. **Research Gap:**
   When implementing an ISMS in local governments, in the absence of adapted procedure and implementation models in the broadest sense, reference is usually only made to handouts such as practical guides, measures to create management

attention or simple training and awareness-raising measures (Bostelmann, 2021, p. 188). If at all, measures and instruments to increase resilience are usually considered in isolation or only shed light on sub-areas. This approach does not go far enough. The limited view of the big picture only allows limited transferable insights regarding the optimal structure of an information security management system in small local governments.

1.2 Aim and Research Objectives

The contribution of the present research to its scientific discipline and, simultaneously, the result of a creative research approach lies in developing an integrated procedural model for establishing an information security management system in small local governments. Information security management is integral to an organisation (Sowa, 2017, p. 17).

From a technical point of view, many solutions already exist today that can significantly improve the security of the information infrastructure. At the conceptual level, there are solutions for managing, implementing and monitoring information security. There are national and international specifications and standards, such as those of the German Federal Office for Information Security (BSI) and the International Standard Organization (ISO/IEC).

However, the sectoral view must give way to a holistic view to implement information security effectively and efficiently. Information systems are socio-technical systems that can only perform their tasks in cooperation with humans. These socio-technical systems function differently in profit-oriented organizations than in public administration.

The main aim of the present thesis is to determine and present the peculiarities of local government. At the same time, assess their influence on establishing information security management systems. The main objective of the present research work will be achieved if it is possible to develop and prove an integrated procedural model for creating and establishing an ISMS that can be used by small local governments and is also practical.

Against this background and the research gaps described in the problem definition addresses the following research objectives:

The **main objective of the findings** is divided into the following research objectives:

A1. Determination of the status quo of information security in small municipal administrations.

A2. Determination of the characteristic features of local government.

A3. Determination of the unique requirements, framework conditions and architectures for developing and establishing an ISMS in municipal administration.

The **design part** of the thesis focuses on the following research objectives:

B1. Determination of the main stakeholder groups for consideration in the process model.

B2. Determination of relevant activities of the process model.

B3. Development of a software prototype to support the implementation of the procedural model.

These research objectives are answered with the help of the publications (section 5 to 11) and in the course of this work.

1.3 Overview of the current State of Research

Information technology has changed a lot in the last 30 years. At the beginning of development, computers existed as mainframe computers, to which only specialized personnel had access (von Solms, 1996, p. 258). In the 1980s, miniaturization brought personal computers (PCs) into companies and administrations for the first time. In a further step, these PCs were then successively connected by local networks, thus establishing distributed data storage and processing. Although employees outside the IT department now also worked with PCs, data storage and access to the information systems remained within the organization.

This picture changed with the innovation of the "Internet" at the end of the 1980s. The borders have since dissolved. After the initial use of services such as e-mail and simple websites, companies and administrations are increasingly networking within the framework of business-2-business relationships. Furthermore, the customer-driven tendency towards business-2-customer relationships has been observed in recent years. The range of IT systems and their possible uses has expanded rapidly. It extends from the original server room with mainframe systems to entire corporate networks and beyond these boundaries. Today, mobile workplaces and home offices are almost the standard in all industries (Martin et al., 2022).

The responsibility for the information systems per se and the information processed with them has changed due to this change in reach. As IT technology increasingly moved into the individual business units, responsibility shifted more and more from the original IT specialists up the hierarchical level to the management of the organization (von Solms, 1996, p. 258).

Furthermore, the ubiquity of information systems also impacts security management. *SOLMS* identifies three stages of the development of information security (von Solms, 2000):

The **first** stage was more of a technical treatment of information security, focusing on access monitoring, user identification and passwords.

The Internet innovation characterizes the **second** stage. The associated and steadily increasing electronic business traffic catapults information security onto the tables of upper management. As a result of the second stage, information security policies, organizational structures and the function of the information security manager were created. The first security standards, such as those of the Federal Office for Information Security (BSI), were developed during this time. This was accompanied by a fundamental improvement in information security, which, however, tended to focus on large organizations due to its history. Due to the increasing dependence on IT, both for companies and administrations, the procedures developed in the second stage must be further developed and adapted to the target group's needs.

These adaptations are researched in the **third** stage and try to answer questions such as developing process models, standardization, certification and metrics for measuring success as a basis for continuous improvement. At the same time, the third stage, which continues to this day, also focuses on the socio-technical dimension, which is probably the most significant challenge in implementing information security (von Solms, 2000).

Further research sheds light on different areas of information security, which are briefly summarized below and are divided into several segments (legal, social, organizational and technical research areas):

Following *Solms*, the authors *Glaspie* and *Karwowski* focus on these **human factors** in information security culture in their study and found that the human factor is always the weakest link in the enforcement of measures and that this aspect needs to be optimized (Glaspie and Karwowski, 2018). The influence of the **human factor** on information security has also been studied by *Benson* et al. It was found that personality factors, awareness, norms and cultural context significantly influence information security in organizations (Benson et al., 2019).

In contrast, *Jalali* et al. examine the **organizational** perspective of information security in the U.S. healthcare sector and try to transfer the results to other areas (Jalali et al., 2019).

Preis and *Susskind* also make similar observations. At the core of her work is the retrospective analysis of various studies regarding the **status quo of information security** in US municipalities with the following results: Only a minimal number of local governments have developed or established an appropriate information security strategy (Preis and Susskind, 2022, p. 617). Non-existent financial and human resources are cited as obstacles by the municipalities surveyed. Furthermore, risk management is practically non-existent in the local governments studied. To make matters worse, according to *Norris*, many US local governments suffer from permanent cyberattacks. At the same time, they operate their IT infrastructure with poorly trained employees, whereas the management level of these same municipalities rates cybersecurity as "good to very good" (Norris et al., 2019, p. 896).

The authors *CHOEJEY* et al. examined **organizational** success factors for establishing information security in government organizations in Bhutan. The study revealed several factors that are essential for the successful implementation of information security or cybersecurity strategy, namely: Awareness of employees for the ISMS as well as target group-specific training, creation of security policies, provision of the necessary budget, internal security audits, determination of security responsibility, establishment of an appropriate (ISMS) organizational structure, change management as well as communication and cooperation (Choejey et al., 2016).

A study in Polish local governments has shown that not only are financial resources essential for the establishment of information security, but also **qualified employees** play an essential role (Chodakowska et al., 2022). Goodyear et al. researched US companies in a similar direction as early as 2010 and clarified that the **security manager** is essential for setting up an ISMS (Goodyear et al., 2010). Recent studies also confirm this (Nifakos et al., 2021).

AWAN et al. investigated which specific technical measures are used in the context of security strategies (Awan, 2017). The result of the study remains sobering, as it only brings to light platitudes. Similarly*, BARTSCH* and *FREY*, who describe in detail the various threat situations and motive structures of the perpetrators and the course of a cyberattack for the target group administration, also stick to the description of possible measures in general but instead compile an overview of the steps that should be taken after a successful cyberattack (Bartsch and Frey, 2017, p. 83ff).

While the research mentioned above reports focus mainly on only one area of investigation, the work of *TATIARA* et al. sheds light on a broader field of research. As a result, the authors describe the necessary foundations for the successful implementation of an ISMS and identify a total of seven key areas:

1. Involvement of the management level,
2. Information for employees,
3. Regular review of the implementation of the security measures,
4. Communication of the improvement plan,
5. Defining roles,
6. definition of tasks and
7. Create and distribute guidelines and work instructions.

Further research on how the sub-areas must work together to deliver a concrete result was not examined (Tatiara et al., 2018).

Recent research reports have come to similar conclusions. For example, *POEHLMANN* et al. list five essential success factors concerning information security (Poehlmann et al., 2021): **First,** the **technical** aspects, such as the usability of cybersecurity and the **technological** design process and its effects on cybersecurity are examined. **Secondly**, the **management process** is cyclical, starting with identifying, assessing, and responding to risks and ending

with controlling the continuous improvement process. **Thirdly**, it is precisely this management process that must be integrated into an appropriate **organizational structure** to establish strategies to strengthen information security in the company and simultaneously reduce the costs of cyberattacks. **Fourthly,** the effects of the **legal** basis are examined. These, in particular, contribute to awareness of the need for information security in public administrations, as this mainly affects the management level. Finally (**fifthly**), these authors also refer to **human** factors as an essential success factor. Furthermore, the authors demand that in addition to a purely theoretical consideration of success factors, case studies should also be considered to test methods and models more in practice and to draw conclusions from them. Theoretical models and the demand for model development for practical application remain here.

Despite increasing interest from practitioners, information security is perceived in academia as an essentially technical topic (Alguliyev et al., 2018), (Lezzi et al., 2018), (Sallos et al., 2019). Nevertheless, *SOLMS* and *NIEMIMAA* observe that in recent years, **information security standards** and **frameworks** have become increasingly important in implementing ISMS (von Solms, 1999), (Niemimaa and Niemimaa, 2017). These frameworks include ISO/IEC 27001. It was developed jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) based on the "BS 7799-1"[1] standard and was first published in 2005. She "*... specifies the requirements for establishing, implementing, maintaining and continuously improving an information security management system (ISMS) within an organization*". The requirements "*...are of a general nature and should apply to all organizations, regardless of type, size and type*" (*DIN ISO/IEC 27000*, 2016; *DIN ISO/IEC 27001*, 2018).

Overall, there are significant concerns in the scientific literature regarding information security standards such as ISO/IEC 27001 concerning their effectiveness, validation and application (Siponen and Willison, 2009), (Silva et al., 2016), (Niemimaa and Niemimaa, 2017). The high degree of abstraction of ISO/IEC 27001 makes it difficult for organizations to implement quickly and easily.

The German Federal Office for Information Security (BSI) has broken up the high degree of abstraction and developed a catalogue of measures with around 1,800 measures, the so-called "Abstract Measures". **IT Baseline Protection Catalogue**, the implementation of which is described in four framework documents (BSI, 2023; “BSI-Standard 200-1,” 2024; “BSI-Standard 200-2: IT-Grundschutz Methodik,” 2024). As a de facto standard for IT security, IT Baseline Protection is aimed mainly at federal authorities or large organizations.

ISO/IEC 27001 and IT Baseline Protection are increasingly used in companies or administrative organizations. The authors *MARKUS* and *MEUCHE* examined the advantages and disadvantages of these two concepts when setting up an ISMS. They found that the

[1] BS 7799-1:1999 = British Standard 7799-1:1999, which defines a code of practice for information security

established process models are unsuitable for small organizations due to their complexity and scope (Markus and Meuche, 2022, p. 209). **It is precisely this gap that the present work addresses**.

Since the early 2020s, the number of publications in information and cyber security has steadily increased. This is probably related to the further increase in the threat situation and the associated need for research.

However, the work only focuses on marginal areas such as technical security measures, employee awareness or legal discussions in the context of the NIS 2 Directive. Due to existing established standards, e.g. ISO 27001 or BSI baseline protection, no further research is likely to take place to develop **lean** solutions for small to medium-sized organizations that are tailored to their requirements and, above all, to their financial, personnel and organizational framework conditions in terms of scope, complexity and resource requirements.

It is incomprehensible why this field of research, in particular, has been so little researched, as 85% of local governments in Germany are small administrations located in places with fewer than 10,000 inhabitants (“Destatis,” 2024).

The status quo is usually quantitatively surveyed in existing studies, and gaps and hurdles are roughly identified. Therefore, the group of small and medium-sized local governments is examined in this thesis to gain insights into why the establishment of information security is not the focus of those responsible and which barriers could be accountable for this. This thesis pursues further advancing information security research in small municipal organizations by partially or entirely closing gaps.

1.4 Research Design and Research Methodology

1.4.1 Design Science Research as a Research Paradigm

The present work focuses on a design research goal. The process model "Design Science Research (DSR)" from *HEVNER* is suitable for investigating the practice-relevant challenges in developing a procedural process model for creating and establishing an ISMS in small administrative organizations and developing appropriate solutions.

According to *HEVNER*, a process model to be developed is an artefact in the sense of the design-oriented research paradigm (Hevner et al., 2004, p. 76). Design-oriented research does not aim at the ultimate truth in quantitatively testable causal relationships but focuses on proving its usefulness. Furthermore, *HEVNER* points out that the behavioural science and the design-oriented research paradigm cannot be separated from each other; they go together like horse and carriage (Hevner et al., 2004, p. 77).

The design-oriented research results in constructs, models, methods and instantiations (Peffers et al., 2006), (Recker, 2021, p. 102). *Wilde* and *Hess* state that design-oriented research covers most research in business informatics (Wilde and Hess, 2006). Case study research is predominantly conducted in the German and Anglo-Saxon worlds. In the Anglo-Saxon world, behavioural research methods such as case studies or quantitative empirical analysis are most commonly used (Peffers et al., 2006, p. 84), (Wilde and Hess, 2006, p. 285). Works that pursue a design-oriented approach have been underrepresented there in the past (Peffers et al., 2006, p. 84).

This imbalance has led to a controversial debate about the quality of scientific results (rigour) and practical relevance (relevance) (Benbasat and Zmud, 2003). As a result of this debate, the methodological profile was sharpened in the German-speaking and Anglo-Saxon worlds, which led to the realization that valid and practical research results can only be achieved through combining both research paradigms (Hevner et al., 2004).

To classify and better understand design science research, *Hevner* et al. have defined a framework with which the authors significantly contribute to sharpening the design-oriented research approach (Hevner et al., 2004), (Recker, 2021, p. 106ff). With this framework, the Design Science Research approach is directly related to the environment and the knowledge base (Figure 1).

First and foremost, the **environment** defines the problem to be solved with the help of the artefacts to be developed. This environment consists of the components of people, organizations, and the tasks and technologies that interact with each other. The knowledge base contains various tools such as scientific theories, methods and frameworks.

This allows the design science research approach to be carried out and artefacts to be generated that are part of the desired overall solution. The actual design science research approach is characterized by recurring development and evaluations of the artefacts using the research methods and tools listed in the table below (Table 2). This ensures a continuous improvement process that focuses on the three pillars of the framework and combines relevance (relevance cycle) and rigour cycle with each development cycle. The figure below illustrates these relationships (Figure 1).

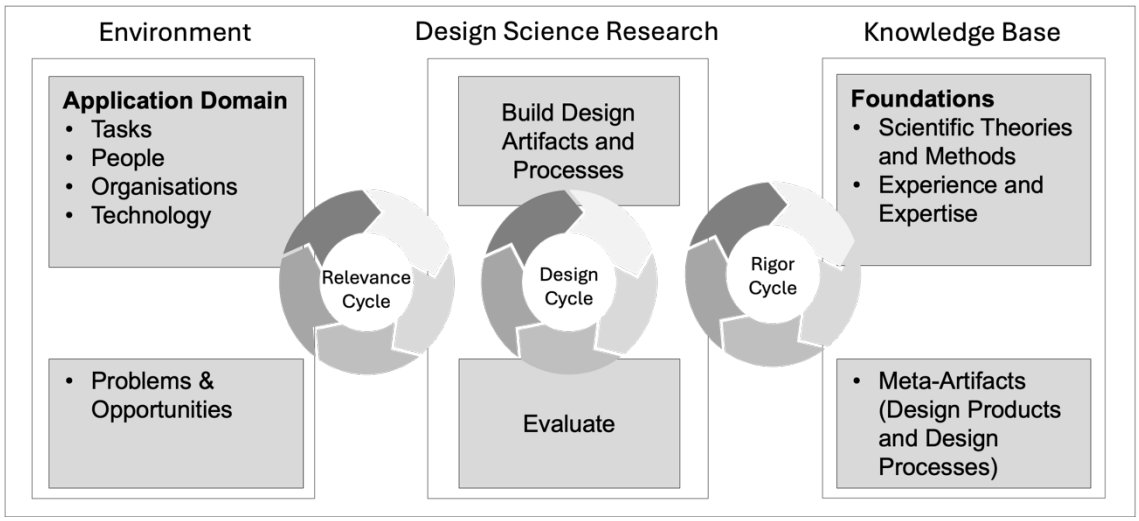

Figure 1: Design Science Research Framework

based on Hevner and Chatterjee (2010, p. 16), Hevner et al. (2004, p. 80)

To further validate a research approach, *HEVNER* et al. recommend that the following seven guidelines be considered when implementing the Design Science Research Approach (DSR) (Hevner et al., 2004, p. 83).

Guidelines for the implementation of the Design Science Research approach:

1. **Design as an Artifact**: Design-science research must produce a viable artefact as a construct, a model, a method, or an instantiation.
2. **Problem Relevance**: Design-science research aims to develop technology-based solutions to important and relevant business problems.
3. **Design Evaluation**: Via well-executed evaluation methods, the design artefact's utility, quality, and efficacy can be demonstrated.
4. **Research Contribution**: Effective design-science research must provide transparent and verifiable contributions in the design artefact, design foundations, and design methodologies.
5. **Research Rigor**: Design-science research relies on rigorous methods in constructing and evaluating the design artefact.
6. **Design as a Search**: The search for a practical artefact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
7. **Communication**: Design-science research must be presented effectively both to technology-oriented and management-oriented audiences.

The first guideline, "**Design as an Artifact**", requires the Design Science Research Process (DSRP) to always be an artefact in the form of a model, method, or instantiation.

With the second guideline, "**Problem Relevance**", *HEVNER* defines that the Design Science Research process should generate solutions for meaningful and relevant problems from practice.

The third guideline, "**Design Evaluation**", ensures that the generated artefacts meet the necessary quality criteria through appropriate evaluations. Different methods from the knowledge base can be used (Hevner et al., 2004, p. 86).

This lays the foundation for the fourth guideline, "**Research Contribution**", which states that the design science research process must generate a transparent and scientifically verifiable contribution.

The fifth guideline, "**Research Rigor**", must be considered to ensure this. The artefact's construction and evaluation must work with precise and established methods from the knowledge base. Essential for assessing artefacts is considering behavioural theoretical approaches (Hevner et al., 2004, p. 88).

When the best artefact is available through iteration from development and evaluation, it is defined by the sixth guideline, "**Design as a Search**". These requirements are followed by the seventh and final guideline, "**Communication**". It describes the necessity of communicating the results to create a basis for feedback from a technological and practical point of view.

The literature describes process and procedure models for implementing the Design Science Research approach based on these guidelines (Hevner and Chatterjee, 2010). The Design Science Research Methodology Process Model by *Pfeffers* et al. is the most frequently cited in the literature. *Pfeffers* et al. have analysed related publications and present their model for implementing the Design Science Research approach, which consists of individual steps summarised in the table below (Table 1), (Peffers et al., 2006, p. 91).

Table 1: Steps of the Design Science Process

Step	Literature
1. Problem Identification and Motivation	(Archer, 1984), (Eekels and Roozenburg, 1991), (Hevner et al., 2004), (Nunamaker Jr. et al., 1990), (Rossi and Stein, 2003), (Takeda et al., 1990), (Walls et al., 1992)
2. Define the Objectives of a Solution	(Eekels and Roozenburg, 1991), (Hevner et al., 2004)
3. Design and Development	(Archer, 1984), (Eekels and Roozenburg, 1991), (Hevner et al., 2004), (Nunamaker Jr. et al., 1990), (Rossi and Stein, 2003), (Takeda et al., 1990), (Walls et al., 1992)
4. Demonstration	(Eekels and Roozenburg, 1991), (Nunamaker Jr. et al., 1990)
5. Evaluation	(Eekels and Roozenburg, 1991), (Hevner et al., 2004), (Nunamaker Jr. et al., 1990), (Rossi and Stein, 2003), (Takeda et al., 1990), (Walls et al., 1992)
6. Communication	(Hevner et al., 2004)

These process steps can be summarized as a process diagram based on Pfeffers as follows (Figure 2), (Peffers et al., 2006, p. 93). Each of the first four activities of the DSR process can represent a possible entry point into the DSR process.

This thesis aims to develop a process model for creating and establishing an ISMS in small administrative organizations. The unique features of the "public administration" research field are not directly recognizable.

Against this backdrop, the starting point for the present research work is the "problem identification" from the *PFEFFERS* process.

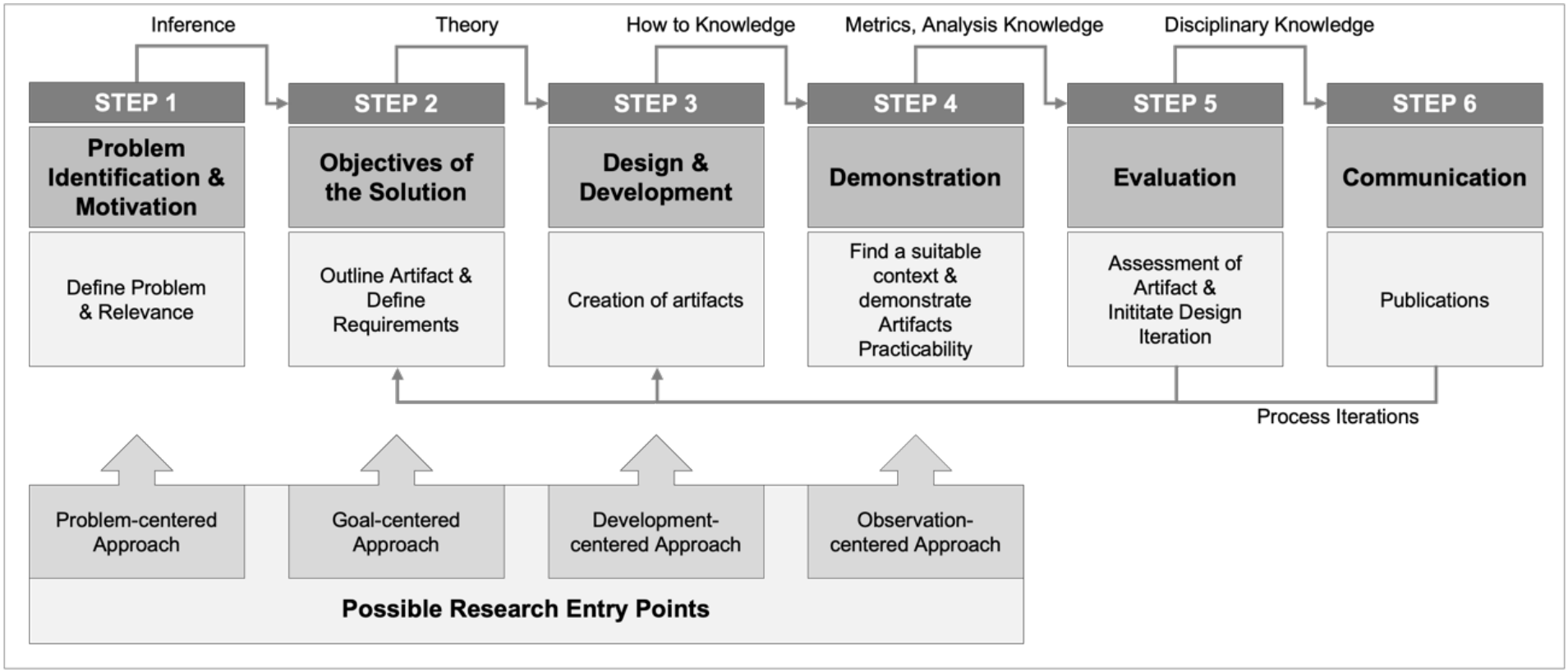

Figure 2: Design Science Research Process (DSR-Process)

1.4.2 Presentation and Selection of Research Methods

As already described in the previous remarks, the present thesis deals with information security. In this context, a procedural model for small local governments is to be developed, and an ISMS can be set up and operated for specific target groups. This goes hand in hand with a tremendous construction-oriented reference to the topic. To meet these requirements, it is first necessary to define one or more research methods oriented towards the objective or the research questions that can contribute to solving the problem.

Choosing a suitable research method depends on several factors: problem and research goal, research framework and analytical methods, and epistemological and ontological assumptions (Becker et al., 2003, p. 5). In this context, a method is generally defined as an approach that uses a specific selection of instruments to achieve the goal. If comprehensible and verifiable rules of conduct describe such an approach, one can generally speak of a research method (Wilde and Hess, 2006). Furthermore, scientific methods are characterised by the fact that they describe the subject area (**descriptive context**), try to gain new knowledge by taking these considerations into account (**cognitive context**) and then substantiate these findings (**reasoning context**) (Heinrich et al., 2011, p. 74ff).

Many different research methods are available for scientific disciplines, such as business or administrative informatics, although it is challenging to assign research methods to scientific disciplines (Lange, 2005), (Becker and Niehaves, 2007, p. 209). This is because the individual methods were developed in scientific research practice and are used by various research disciplines. Restrictions and concretizations result from the particular problem in each case. *Hars, Wilde* and *Hess* have compiled a list of the most frequently used methods in business informatics (Hars, 2002), (Wilde and Hess, 2006).

To list all these research methods at this point would go beyond the scope of this work. The following table provides an overview of the research methods compiled by the authors mentioned above (Table 2). The excerpt forms the basis for a review of whether one or more research methods listed here can be applied to a sufficient extent for the problem of the planned research work. The left column names the research method, the middle column contains a short description, and the right column refers to the literature.

Table 2: Research Methodologies

Research method	Description	Literature
Action Research	A mixed bouquet of methods from science and practice solves a practical problem. Several cycles of analysis, action, and evaluation steps are carried out, each providing poorly structured instruments such as group discussions or simulation games.	(Frank and Lange, 1999), (Rosner and Gombos, 2007)
Ethnography	Ethnography aims to generate insights through participatory observation. The difference between case studies lies in the degree to which the researcher integrates into the social environment under investigation. There is hardly any objective distance.	(Ploder and Hamann, 2021; Wilde and Hess, 2006)
Case Study	The case study usually examines complex, hard-to-define phenomena in their natural context. It represents a particular qualitative-empirical methodology that intensively examines a few trait carriers. The focus is either on the most objective investigation of theses (behavioural science approach) or on interpreting behavioural patterns as phenotypes of the realities constructed by the subjects (construction-oriented approach).	(Robra-Bissantz and Strahringer, 2020), (Benbasat et al., 1987), (Walsham, 2006)
Formal/conceptual and argumentative-deductive analysis	Logical deductive reasoning can take place as a research method at different levels of formalization: either within the framework of mathematical-formal methods, in semi-formal models (conceptual) or purely linguistic (argumentative).	(Roggenbach et al., 2022), (McDermid, 1987),
Grounded Theory	Grounded theory aims at the inductive development of new theories through intensive observation of the object of investigation in the field. The various procedures for coordinating and evaluating the predominantly qualitative data are precisely specified.	(Strübing, 2021)
Laboratory and Field Experiments	The experiment investigates causal relationships in a controlled environment by manipulating an experiment variable in a repeatable way and measuring the effect of the manipulation. The object of investigation is examined either in its natural environment (in the "field") or in an artificial environment (in the "laboratory").	(Kubbe, 2020)
Prototyping	A preliminary version of an application system is developed and evaluated. Both steps can provide new insights.	(Nugraha, 2020), (March and Smith, 1995), (Goldenson and

Research method	Description	Literature
		Gibson, 2003), (Hevner et al., 2004)
Qualitative / Quantitative Cross-Sectional Analysis	These two methods combine survey techniques such as questionnaires, interviews, Delphi methods, content analysis, etc., into two aggregates. They comprise a one-time survey across several individuals, then quantitatively or qualitatively coded and evaluated. The result is a cross-sectional picture across the sample participants, which usually allows conclusions to be drawn about the population.	(Zerres, 2021), (Borchardt and Göthlich, 2009), (Diethelm et al., 2010) (Bortz and Döring, 2006; Heerwegh, 2006; Walsham, 2006; Wilde and Hess, 2006)
Reference Modeling	Reference modelling usually creates simplified and optimised representations (ideal concepts) of systems inductively (based on observations) or deductively (e.g., theories and models) to deepen existing findings and generate design templates for them.	(Becker et al., 2002), (Fettke and Loos, 2002)
Simulation	The simulation formally maps the system's behaviour to be investigated in a model and simulates environmental conditions by assigning specific model parameters. Insights can be gained through model construction and observation of endogenous model sizes.	(vom Brocke et al., 2020)
Systematic Literature Analysis	With the help of a systematized literature analysis, foundations for further research are laid.	(Dibbern et al., 2004; Fettke, 2006; vom Brocke et al., 2009; Webster and Watson, 2002)

Now, it is necessary to analyse whether and which of the methods presented are best suited for working on the problem. Two criteria can evaluate the methods. On the one hand, scientific methods can be classified according to the degree of formalization. That is, whether **quantitative** (numerical) or **qualitative** (linguistic). On the other hand, there is the possibility of **differentiating the methods more in** terms of behavioural science **or more** construction oriented. The construction paradigm analyzes the structure and evaluation of information systems, whereas the behavioural paradigm focuses on behavioural science and organizational analysis (Wilde and Hess, 2006, p. 11). The illustration Figure 3 summarizes the research methods in Table 2 according to these criteria.

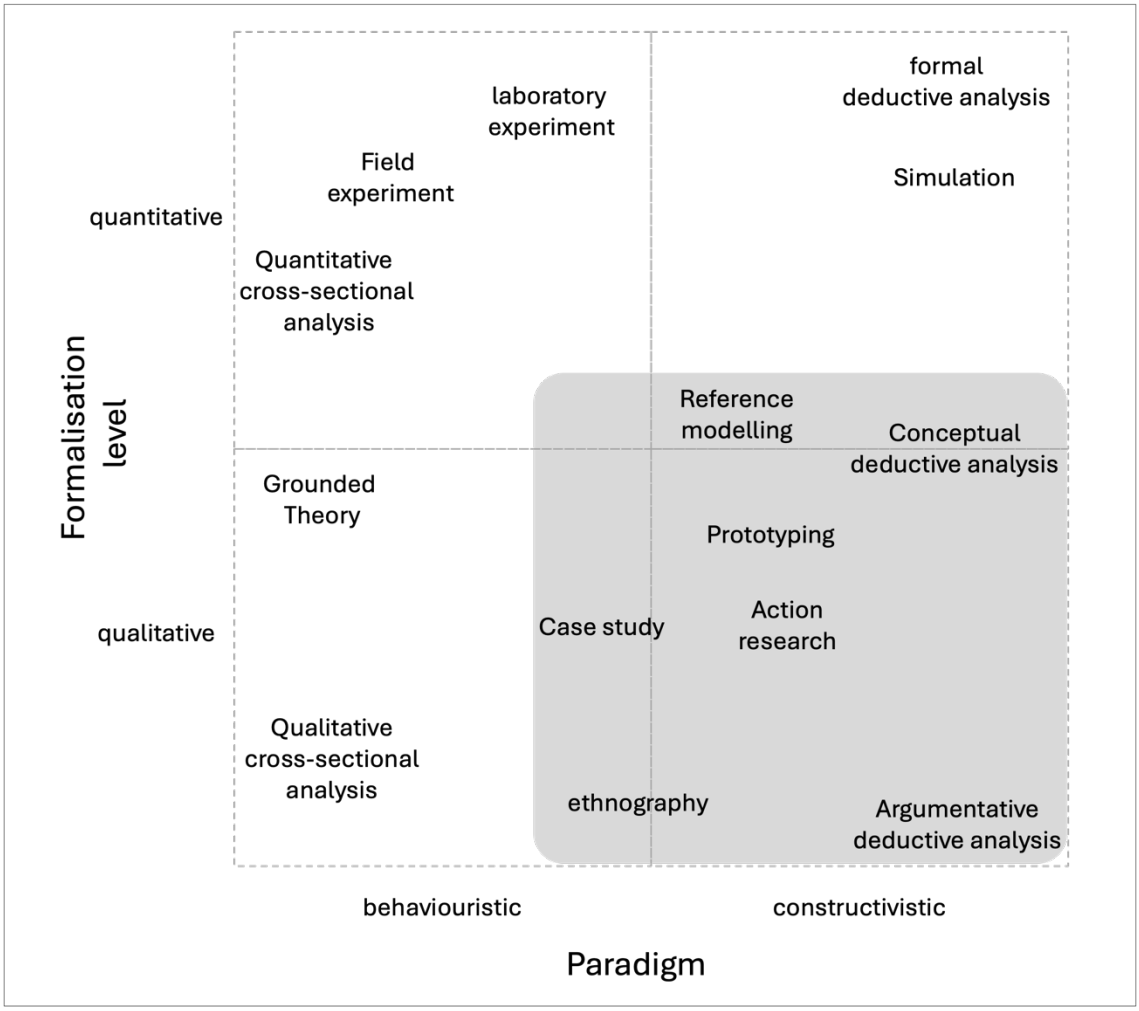

Figure 3: Research Methods

Concerning the problem of the present dissertation, which is to develop a process model for developing and establishing an information security management system in small local governments, it becomes clear that a construction-oriented research method is needed. Nevertheless, no clear dominance can be found for the qualitative/constructivist field, as both quantitative and qualitative methods (interviews and questionnaires) are necessary to evaluate the research work. Laboratory and field experiments also test the research results in controlled and natural environments.

Thus, the selection of possible research methods can be limited to reference modelling, conceptual-deductive analysis, prototyping, case study, action research, ethnography and argumentative-deductive analysis, i.e., a mix of methods has been applied during the research work (Venkatesh et al., 2013), (Österle et al., 2010).

Prototyping, in particular, was considered an essential method for the present research work, as both the process model and software should be available for laboratory and field experiments on time (Preußig, 2018).

The **action research** also formed an essential basis of the research work, as the process model and the software are tested with test clients in natural environments. A necessary

feature of action research is that several cycles of analysis, action, and evaluation steps are run through to develop the existing artefact further (in this case, process model and software) or integrate findings into the improvement.

In this context, it becomes clear why **ethnography** has also been used as a research method. The researcher was very closely connected to the test clients during the research work. Through participatory observation, new insights were generated (e.g. in usability of the software), which were only possible through direct contact with the test subjects.

Since the present dissertation pursues a design research goal, inductive (based on observation) and deductive analyses (gaining knowledge with the help of theories and models) were applied based on **reference modelling** to develop and improve the artefacts iteratively.

To "manage" the methods used throughout the research work, Hevner's research paradigm ", Design Science Research (DSR)", presented in Section 1.4.1, was applied.

1.4.3 Research Methodology and Application of Design Science Research

Further research was carried out with the help of the iterative process of *PFEFFERS* et al. (Benner-Wickner et al., 2020; Peffers et al., 2006), taking into account the guidelines described by *HEVNER* and is described below (Hevner et al., 2004).

This thesis addresses the relevant and complex problem of "**Establishment and Establishment of an ISMS in Small Local Governments**" (Section 1.1 Problem Definition and Motivation). The problem relevance is according to the guideline "**Problem Relevance". Thus**, the first step of *PFEFFERS'* Design Science process is already derived in this chapter and, at the same time, formulated as research gaps.

In preparation for the second step, "**Define Objectives of a Solution**", of the *PFEFFERS* process model, basic requirements and objectives are presented. To this end, corresponding research questions are formulated, which will be answered during the thesis (Section 1.2. Aim and Research). This is done with the help of publications in chapters 3 and 4-10, where the individual publications are compared with the research questions with the help of a regulatory framework.

In addition, according to the guideline "**Design as an Artifact**", a procedural model is developed within the framework of the third step ", **Design and Development**", which supports or simplifies the establishment of an ISMS in a local government and can be understood as a solution to the problem. The development of the artefacts is described in the publications and can be found in chapters 4-10.

Based on the "**Design Evaluation**" guideline, the developed artefact is described in detail in the process steps of demonstration (step 4) and evaluation (step 5) and its functionality is checked. The evaluation methods used, such as field trials, interviews and statistical

analysis, are mentioned and described in the sub-chapters or the publications (chapters 4 to 10).

Last, the sixth process step, "**Communication**", is fulfilled by the present work. In addition, the requirements of the "Communication" guideline are met on the one hand through close support of the test clients and an active exchange of information with the users of the process model. On the other hand, through the presentation and publication of further research results from this work in journals (e.g. DuD, HMD-Praxis der Wirtschaftsinformatik).

1.4.4 Structure of the Thesis

The structure of the thesis is presented as a building with floors and a foundation with the DSR process (Figure 4).

The guidelines of the Design Science Research approach are used as the foundation of the building, as the research work was carried out according to these guidelines.

In Part A (1st Floor) of the thesis, the research questions and research methods are described in the introductory chapter. This is followed by Chapter 2, in which the basics are described, and the necessary definitions are carried out. This essentially includes a description of the structure of local government that is better able to open up the field of research to the reader. This is followed by further definitions of terms (1st Floor Figure 4).

In the second part B (2nd floor) an overview of the literature already published is provided first. Subsequently a research methodological classification takes place for the author's selected number of publications. Subsequently, the listed research questions are assigned to these publications and the design science research process before the publications are listed in detail (2nd Floor Figure 4).

The following chapter in Part C (3rd Floor) provides insight into the software that supports the procedural model developed in the present work.

Part C (4th Floor) summarises the results in the last chapter of the thesis, as well as the implications for science and practice. In addition to the limitations, the desideratum presents the need for further research.

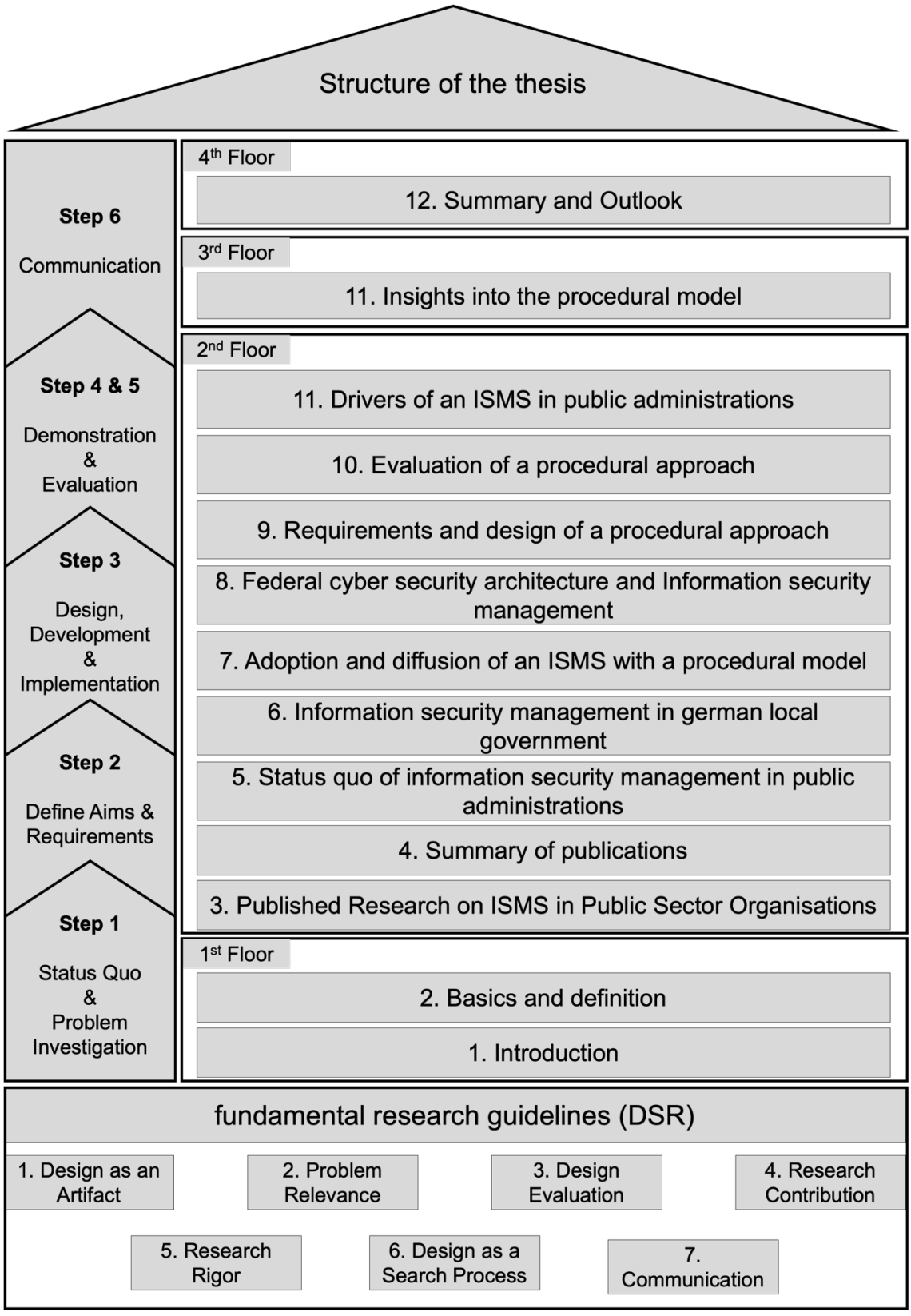

Figure 4: Structure of the thesis

1.5 Research Relevance

The **demands of stakeholders** on the provision of services by the administration have changed significantly in recent years. Digitization has created new needs among some stakeholder groups (Meuche, 2022, p. 100). With increasing digitalization, questions about digital technologies' security are increasingly becoming a focus (Meuche, 2022, p. 100), (Braun, 2021).

As a result, the legal requirements for ensuring IT security have changed considerably in Germany and the EU in recent years. This is accompanied by various reform documents, such as the IT Security Act 2.0 (ITSiG 2.0) from April 2021, the Cybersecurity Act, which came into force in 2019, and the EU Directive with measures to ensure a high level of shared network and information security (NIS-2), which has been in force since 2016 (Schünemann, 2020, p. 8), (Weissmann, 2023).

These reform documents are not an end in themselves, but define cyber and information security measures and, at the same time, raise awareness of cyber security among the responsible. This is especially true against the background that the **number of cyber-attacks** on infrastructures of companies as well as administrations or critical infrastructures has been increasing for years (Schreiber, 2022, p. 238), (Dreißigacker et al., 2021, p. 52).

Environmental dynamics such as the COVID-19 pandemic have led to a further **push for digitalization** with opportunities but also risks (Jäggi, 2023, p. 153f). At the same time, the war of aggression in Ukraine has further exacerbated the security situation for both companies and administrations (Schünemann, 2020, p. 10), (Jäggi, 2023, p. 178).

The community, i.e., citizens and companies, has an increased interest in ensuring that the tasks performed by municipal institutions are carried out "**safely**" (Schreiber, 2022, p. 237). This includes the usual administrative services such as issuing an identity document and tasks such as ensuring the water supply.

Furthermore, data and information are increasingly becoming essential resources and must be protected accordingly (Engländer et al., 2022, p. 373). The same applies to administrations, as they are also increasingly processing and storing digital data. Due to the increased networking of information technology, the greater openness due to data-driven services and related legal requirements, information theft, data manipulation and data loss are increasingly becoming administrations' focus (Engländer et al., 2022, p. 374).

The increasing number of **successful cyber-attacks** on administrations also makes it clear that a rethink or better proactive actions are also necessary for administrations to increase cyber resilience (Knodt and Platzer, 2023, p. 8).

Local governments have become a **critical success factor in cross-network cybersecurity architecture**. They are increasingly victims of successful cyberattacks, as the topic of cybersecurity is not or cannot be addressed by the management level due to

personnel, organizational, technical and financial challenges (Moses and Rehbohm, 2023a, p. 648).

At the same time, small local governments face as much risk as large organisations but are more vulnerable at any given time due to reduced resources (Alahmari and Duncan, 2020, p. 2).

The existing approaches and process models regarding information security are unsuitable for small administrative units due to their complexity (Markus and Meuche, 2022, p. 209). In German local government, 35% (=3,779) of local authorities are located in municipalities with fewer than 1,000 inhabitants and usually have fewer than 20 employees ("Destatis," 2024), (Schmid, 2019, p. 102). Information security is not the core business of the range of tasks in such municipalities but a necessary evil.

Literature sheds light on many individual topics but does not provide an overall view. The following gives a brief overview:

- **Awareness of Employees** ((Benson et al., 2019; Chodakowska et al., 2022; Choejey et al., 2016; Glaspie and Karwowski, 2018),
- **Business Continuity** (Jalali et al., 2019),
- **Application Security** (Çubuk et al., 2022),
- **Training Measures** (Alkhudhayr et al., 2019; Cooke, 2017; Schmitz-Berndt and Chiara, 2022; van Steen and Deeleman, 2021),
- **Emergency Planning** (Jalali et al., 2019),
- **ISMS-tools** (Nikolova, 2017; Sabtu and Mohamad, 2021),
- **Maturity Models** (Clemith and Sicker, 2014),
- **Technical Security Controls** (Glaspie and Karwowski, 2018),
- **Security Culture** (Glaspie and Karwowski, 2018; Khansa et al., 2017),
- **Expertise of Employees** (Chodakowska et al., 2022; Forrester et al., 2022; Poehlmann et al., 2021; Preis and Susskind, 2022),
- **Management Attention** (Arbanas and Žajdela Hrustek, 2019),
- **Security Strategies** (Awan, 2017),
- **Cyber Security Architecture** (Nather, 2018; Taddeo, 2019)**,**
- **Obtaining Information on a Cyber Topic** (Chainey and Alonso Berbotto, 2022; Gedris et al., 2021; Potter and Hurley, 2020)**,**
- **Risk Management** (Kitsios et al., 2022; Susukailo et al., 2022)**.**

However, these are only selective solutions. There is a lack of combining the presented solutions into an overall concept.

Against the backdrop of the challenges listed here, it becomes clear that there is an urgent need for action in implementing information security in small administrative units and that appropriate tools are needed. What is required is a simple process model that can be

quickly implemented in local governments and tailored to the local government's core requirements.

This thesis develops such an overall concept for small local governments in the form of a process model and supporting software.

2 Basics and Definitions

2.1 Administration

2.1.1 Structure of the Local Government

The "municipal" level in Germany represents the lowest level of the federal structure. It includes both municipalities and districts and, for example, in Bavaria, administrative districts (Schreiber, 2022, p. 238) or local districts (Kersting and Kuhlmann, 2018). Germany had 10,786 municipalities as of 31.12.2022 (“Destatis,” 2024). 85% (=9,169) of these 10,786 municipalities have 10,000 inhabitants or less. If the circle is even narrower, there are still 35% (=3,779) municipalities with 1,000 or fewer inhabitants. (“Destatis,” 2024). Their core administrations are often smaller than 20 employees (Schmid, 2019, p. 102).

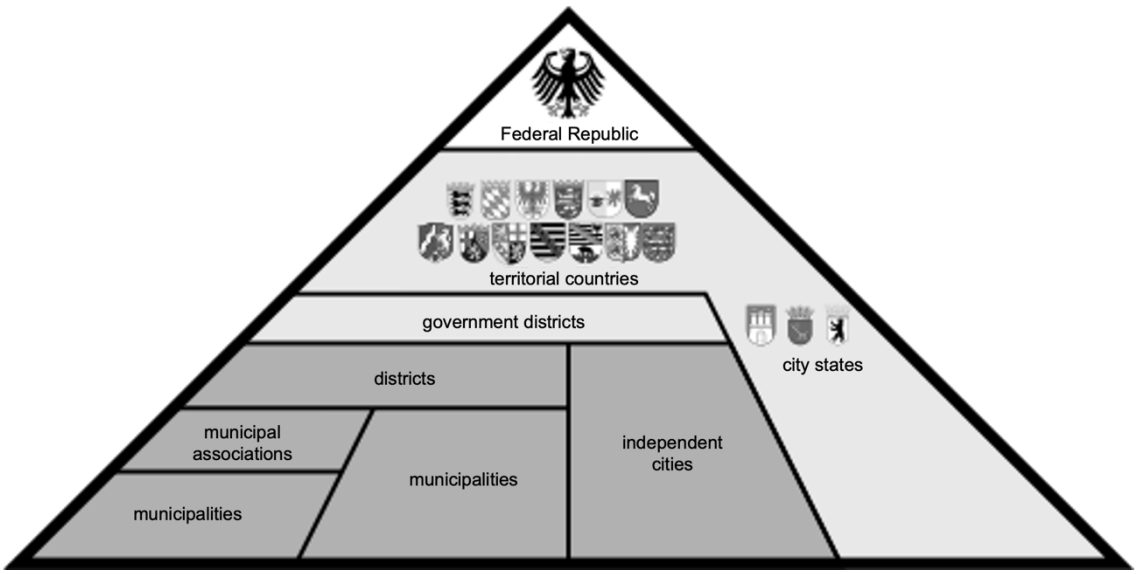

Figure 5: Federal structure of the Federal Republic of Germany

The municipal level has its legal origin in the federal network of the Federal Republic of Germany in Article 28,2 of the Basic Law, which regulates the so-called local self-government:

> „The municipalities must be guaranteed the right to regulate all matters of the local community within the framework of the law on their responsibility. Municipal associations also have the right to self-government within the scope of their statutory area of responsibility, following the law. The guarantee of self-administration also includes the basics of financial self-responsibility; these bases include an economic power-related tax source to which the municipalities are entitled with the right of assessment“.

This means that municipalities are generally granted the right to fulfil their tasks within the framework of cooperation with other public or private actors within the framework of a partnership or on a contractual basis (Windoffer, 2018, p. 371).

At the state level, the **right to self-government** is constitutionally secured in the Local Self-Government Act and in the constitution of the respective federal state (Bogumil and Jann, 2020, p. 123ff). In the context of the municipalities, this means that they have, in particular, statutory sovereignty, personnel sovereignty, financial sovereignty, planning sovereignty, organisational sovereignty and administrative sovereignty for their interests (Bogumil and Jann, 2020, p. 75ff).

However, the municipalities also have to perform specific tasks in addition to the right to self-government. The so-called **commissioned matters** include registration law, building supervision law, immigration affairs, civil defence and regulatory law. Areas of responsibility are motor vehicle registration, foreigners, passport and registration systems, food monitoring, school supervision or trade law. In this area of indirect state administration, there is no room for manoeuvre for the municipalities in shaping the goals (Bogumil and Jann, 2020, p. 121).

Figure 6: Municipal tasks

The following ideal-typical organizational chart can be derived from the municipality's self-government tasks and commissioned matters (Figure 7).

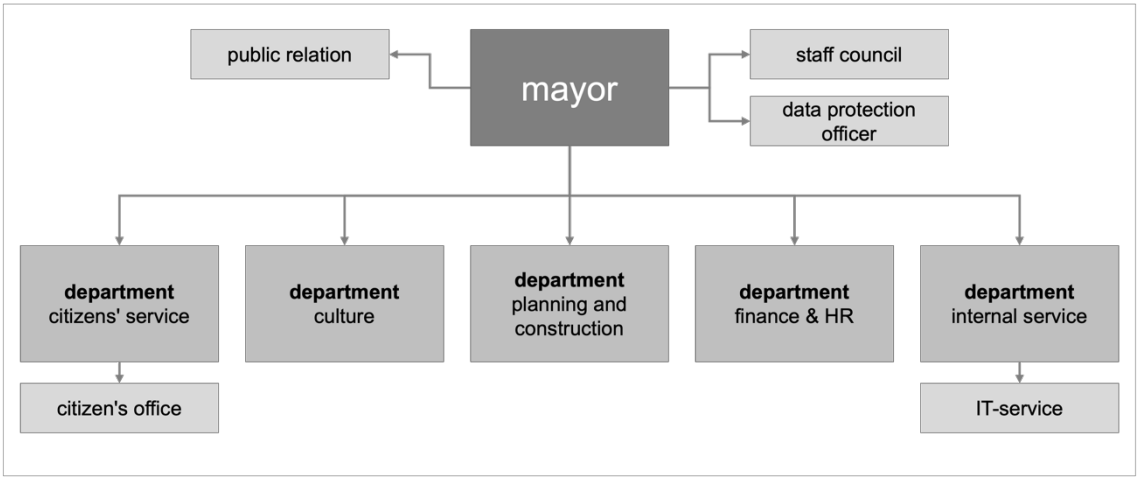

Figure 7: Ideal-typical organizational chart of a municipality

The mayor is at the centre of the administration. Subordinate to him are the departments responsible for self-administration tasks and commissioned matters. Legal requirements require that certain bodies, such as the staff council and data protection officer, be included in the organisational chart (Calder, 2018, p. Art. 37-39).

Due to the decentralised responsibility for organisational issues, which are derived primarily from federalism, the departmental principle and, in particular, local self-government, a very heterogeneous landscape for data and information technology has developed in German federal, state and local administration (Heuermann et al., 2018b, p. 29). At the same time, it is observed that the topic of IT strategy is not a high-priority area of responsibility (Figure 7).

However, digitization and the associated technical possibilities could also lead to changes here in the future. If the technical execution of municipal tasks can be carried out centrally and is also the economically more sensible alternative because it is more cost-effective, the boundaries can become blurred. So perhaps there could be a change from self-administration to self-responsibility in the future. This is because territorial delimitation can no longer be achieved in the electronic space. Since neither a claim to the establishment of isolated solutions nor a compulsion to use central services appears to be a good solution, the principle of cooperation and establishing regional service centres could be a conceivable approach (Bernhardt, 2018, p. 17).

The lack of IT integration as a strategic task at the management level makes it challenging to implement an ISMS in small local governments (Gulden, 2018, p. 141).

2.1.2 IT Planning Council

Through the development of new control mechanisms for public administration (New Control Model – NSM, NPM – New Public Management), the rigid requirements regarding

administrative management have been broken up (Jann, 2019, p. 128). There are no barriers to using modern methods and instruments, which have been successfully used in profit-oriented companies for some time (Schardt, 2017, p. 234). As a logical consequence, the public sector began to digitize administrative processes and the IT Planning Council was set up on 1 April 2010 as a central body for central planning and coordination for federal cooperation in information technology (Figure 8) (Heuermann et al., 2018a, p. 24). Although the IT Planning Council is regarded as the central steering body for the IT of the federal and state governments, its impact extends beyond the cooperation between the federal and state governments and municipalities (Schardt, 2017, p. 228).

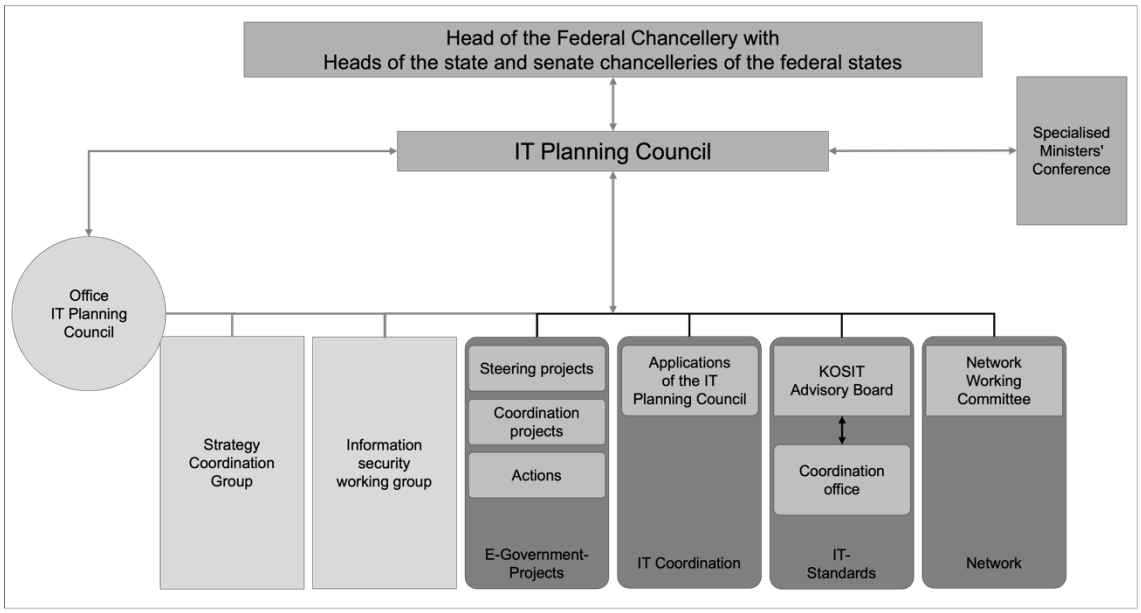

Figure 8: Committees of the IT Planning Council of the Federal Republic of Germany

The main focus of the federal, state and local governments is handling administrative matters. The IT Planning Council is programmatically oriented towards cross-sectional functions to plan and coordinate recurring and similar IT tasks in all departments (Figure 9).

The tasks of the IT Planning Council include the following topics:

- Coordination of cooperation between the Federal Government in matters of information technology
- Decision-making on IT interoperability and IT security standards
- the management of e-government projects
- the planning and further development of the connection network

The "Information Security" working group, composed of 16 state representatives and the federal government, deals with information security issues. This is due, on the one hand, to the increasing digitalisation of administrative processes and, on the other hand, to the growing networking of administrative infrastructures via the interconnection network and the associated dangers and risks for all network users.

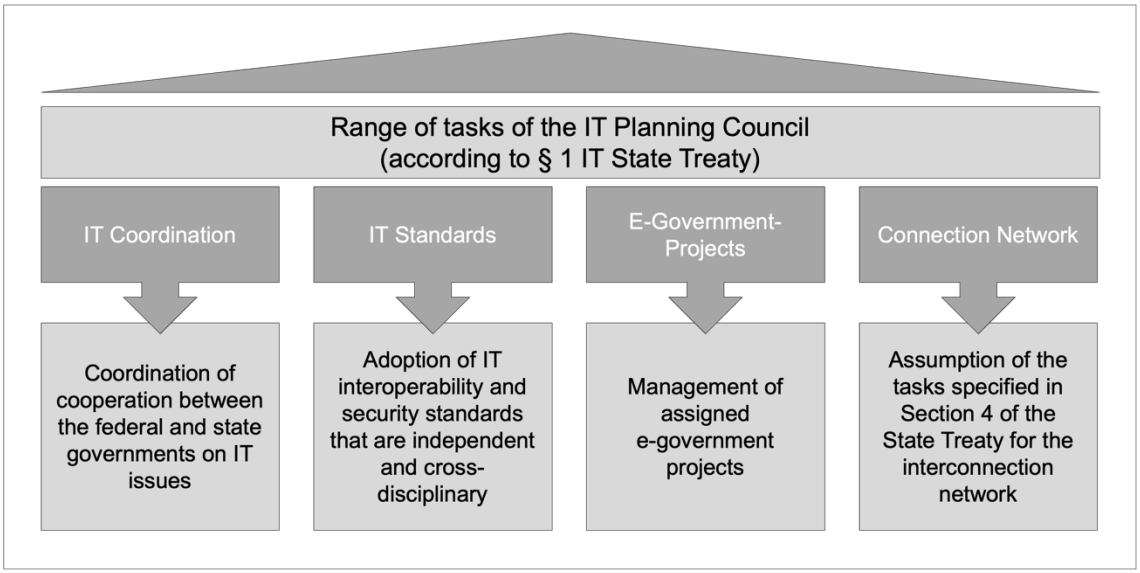

Figure 9: Tasks of the IT Planning Council

In principle, it also applies to all levels of the federally structured public sector that information management, including information security, is not only a critical success factor for operational information and communication technology (IT) but also represents the innovation driver per se.

Against this backdrop, it is even more surprising that since the founding of the IT Planning Council on April 1, 2010, and the publication of the guideline for information security, including the implementation plan on March 8, 2013, the implementation of this guideline has fallen far short of expectations, especially in the municipal sector. For example, only two states (Bavaria and Saarland) have established funding projects by the state government to provide financial support to the municipal family for the development and sustainable establishment of information management and information security management systems (ISMS). In addition to the fact that public administration in the area of planning, implementation and use of IT and related processes is characterized in particular by the importance of the implementation of laws, there is the assumption that there is a lack of suitable approaches, architecture or reference models for the development and establishment of an information security management system in local government that are adapted to the local needs (organizational, technical, personnel and financial).

The tasks of IT governance for the implementation of digitalization and its safeguarding (information security) are supported by several publicly available and partly proprietary "best practice" reference models and standards. *JOHANNSEN* and *GOEKEN* provide a good overview with their analysis and comparison of the reference models (Johannsen and Goeken, 2011, p. 255ff). The aim is to determine which are best suited to the municipal administration to build up and sustainably establish information security management there or whether a new procedural model needs to be developed.

2.1.3 Digitization per se and in Administrations

Digitization efforts have been underway in business and administration for several years. This progressive penetration of digital technologies also entails changes to processes and organizations (Albayrak and Gadatsch, 2017, p. 1683). The term digitization now dominates almost all areas of daily life. This fact is confirmed by the annual report "D21 Digital Index". According to the study, 84% of Germans were already online in 2018, i.e. they use digital services via the Internet. Although the age group of 14 to 29-year-olds is almost entirely digital at 99%, the group of over 65-year-olds is still underrepresented at 48% (Initiative D21, 2019).

If the term "change" is examined in this context, it is noticeable that the German administration is lagging the trend here. Moreover, public administration stands for consistency (Seibel, 2018, p. 1285). The digital transformation changes behaviour and culture (Mergel, 2020, p. 36). Therefore, cultural change is often spoken of in this context.

Digitization is often referred to as a technical revolution, just as industrialization or the development of the steam engine were in their day (Arreola González et al., 2016, p. 7). *SCHUMPETER* describes the further development of a system, e.g. an industry, exclusively as endogenous so that innovation processes can only be brought about by members of the system (Schumpeter et al., 2002). "Groundbreaking" innovations are often created as an innovative adaptation to an external shock such as the COVID-19 pandemic (Mast, 2017, p. 27).

As early as the 1920s, *KONDRATJEV* analyzed five economic cycles triggered by a new need and solution-oriented fundamental innovation. In doing so, he focuses solely on innovations that underlie a technical foundation, thus putting technology in the foreground. *KONDRATJEV'S* findings illustrate the importance of innovation for the development of an industry and the overall economic development (Table 3). However, *SCHUMPETER* makes it clear that it is not only the fundamental innovation that is decisive for evolution, but rather its dissemination and diverse application (Weber, 2004, p. 94f). Information and communication technology (ICT) has precisely this advantage of broad economic and social applicability and, due to its enormous development in recent years, now supports complex problems and provides assistance for various applications (Arreola González et al., 2016, p. 7).

Table 3: Kondratjew'sche Zyklen

Cycle	Year	Description
1. Cycle Steam engine	approx. 1780 to 1840	Early mechanization with the beginning of fundamental innovation: **Steam engine**
2. Cycle Railroad	approx. 1840 to 1890	Second industrial revolution with the breakthrough of the railway Basic innovation: **Railroad**
3. Cycle Electrical engineering	approx. 1890 to 1940	Construction and use of heavy machinery with the breakthrough of electrical engineering Basic innovation: **Electrotechnology**

4. Cycle Automation	approx. 1940 to 1990	Age of automation with the combination of automation and industrialization Fundamental innovation: **integrated circuits, nuclear energy, transistor, computer, car**
5. Cycle Information technology	approx. since 1990	Information and communication age with a breakthrough of digital technology in the face of increasing globalization Basic innovation: **Computer / Network**

Source: (Wächter, 2017, p. 449f)

While *KONTRATJEW* focuses on technology, today's digitalization looks at internal processes and the external interfaces of companies and administrations from a data-driven perspective (Oswald and Krcmar, 2018, p. 7). This change of perspective is accompanied by disruption. This means that something existing can be replaced, displaced, or even destroyed by something new (Arreola González et al., 2016, p. 7).

As a result of digitalization and the associated increasing penetration of digital technologies into the economy, administration and society, the challenges for companies and administrations are to make their business models future-proof (digital business), to continuously adapt organizational structures and processes to changing business models and framework conditions (security) (digital transformation) and to make the best possible use of the potential of new technologies (digital disruption) and to protect them (Figure 10). At the same time, the graphic makes it clear that digitization plays a role not only in the technical infrastructure but also in the processes, the applications, the data processed with them, and the interfaces to the outside. These five levels must be safeguarded in their function by appropriate measures.

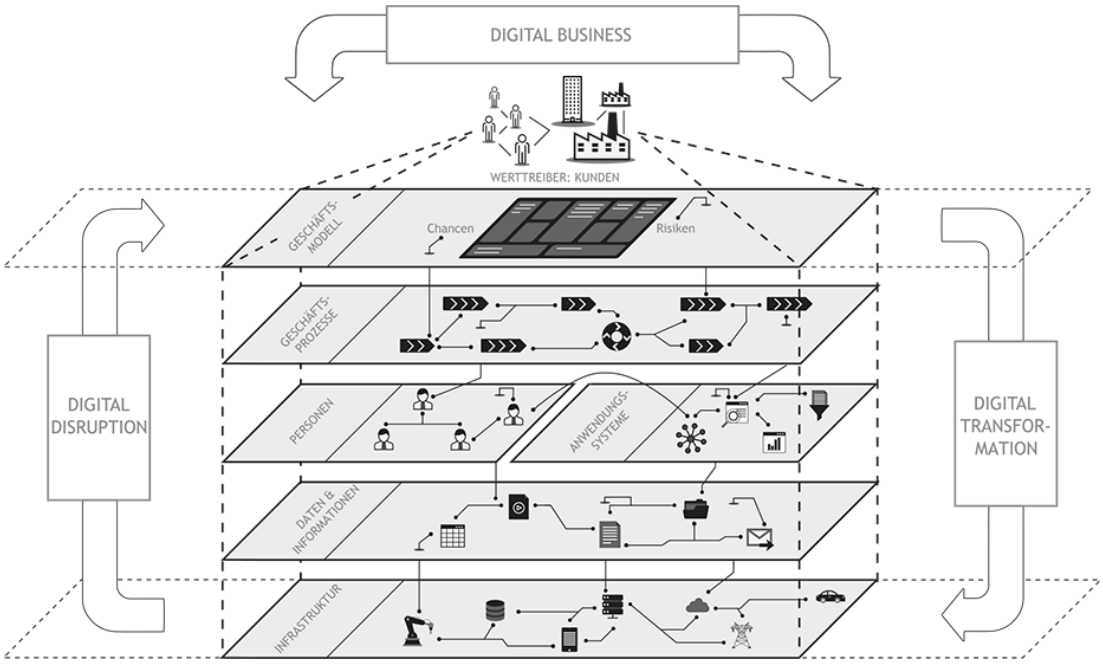

Figure 10: Digitisation

Source: (FIT, 2024)

OSWALD and *KRCMAR* describe this digital revolution by four characteristics (Oswald and Krcmar, 2018, p. 5):

- Inevitability,
- Irreversibility,
- Speed
- and Uncertainty

Inevitability means that social trends such as demographic change will present everyone with significant challenges (especially public administration) that cannot be met without innovative options (Oswald and Krcmar, 2018, p. 7).

The **irreversibility** means that users of digital innovation are no longer willing to do without the gain in comfort they have gained (Oswald and Krcmar, 2018, p. 8).

The **speed** of change is influenced, in particular, by reduced costs for IT infrastructures (Oswald and Krcmar, 2018, p. 8).

The **uncertainty** is explained by the fact that it is difficult to make predictions despite the inevitability. The dynamic change in technologies and industries and the necessity of choosing a technology also bring with it an opportunity for business change. Not every technological trend needs to be followed. It is more critical that organizations put themselves in a position to make the necessary changes at any time, as digital transformation is less a fad than a permanent trend (Oswald and Krcmar, 2018, p. 9).

For public administrations, digitization also brings challenges that, if tackled correctly, also open up opportunities due to the possible changes (Martini et al., 2016, pp. 4–6). Furthermore, administrative action is no longer conceivable today without IT support. This influence of technology will continue to intensify in the context of digital transformation and, at the same time, also harbours one of the risks associated with digitalization, namely the security aspect (Schenk and Dietrich, 2018, p. 268).

One accelerator that helps to master these challenges is the Online Access Act.

Adopting the Online Access Act (OZG) on 18.08.2017 obliges the federal and state governments to provide online access to administrative services by 2023. The Online Access Act (OZG) in Germany was introduced to drive the digitization of the administration and provide citizens and companies with easier and digital access to public administration services. This also directly affects the municipalities that offer a large number of these administrative services (*OZG - Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen*, n.d., p. §1 Abs. 1). The main objectives and advantages of the Online Access Act for the administration are:

- **Digital accessibility**: The OZG aims to make all administrative services of the federal states, municipalities and the federal government digitally accessible by 2022. Citizens and companies should be able to deal with their concerns online without appearing in person (von Lucke, 2021, p. 128).
- **Uniform standards**: The law creates uniform standards and interfaces to ensure interoperability between the different administrative levels. This is intended to make digital offerings more user-friendly and efficient (Seckelmann and Brunzel, 2021a, p. 7).
- **Citizen portals**: Public administration is encouraged to set up uniform citizen portals through which citizens can access digital administrative services. These portals are intended to provide a central access point for various requests (von Lucke, 2021, p. 134).
- **E-Government-Infrastructure**: The OZG promotes the development of a secure and efficient e-government infrastructure. These include, for example, secure identification options (e.g., the electronic identity card) and the guarantee of data protection standards (Brunzel, 2021, p. 342).
- **Accessibility**: Digitization should also benefit people with different needs. Therefore, the OZG calls for the implementation of barrier-free digital services to ensure the participation of all citizens (Lühr, 2021, p. 113).
- **Modernization of the administration**: Digitization is intended to make administrative processes more efficient and transparent. This can help save resources and improve citizen service (Markus and Meuche, 2022, pp. 2, 13, 16).

Therefore, the Online Access Act is an essential step towards modernizing public administration in Germany to offer citizens and companies modern and efficient options for accessing administrative services (Wimmer, 2021, p. 146).

However, the implementation of the OZG is proving difficult (Boos et al., 2023, p. 119). The Covid-19 pandemic, in particular, has highlighted the deficits associated with digitalisation (Hornbostel et al., 2022, p. 37ff).

Attempts have been made to respond to the deficits by investing in digital infrastructure. However, digitalisation problems cannot be solved by using new technologies alone. A deeper analysis shows that the established system of German administration no longer meets the current challenges in various respects. This begins with the question of what the administration should do for which stakeholder groups in the future (digital business). The necessary processes and data flows are derived from this and must be implemented in corresponding administrative structures.

The structures must support the processes in the best possible way and be designed in such a way (digital transformation) that they enable rapid adjustments to changing framework conditions (digital disruption). Finally, managers and employees are needed who can implement the processes efficiently and effectively and develop solutions quickly

when new challenges arise (Hopp, 2020, p. 209ff). This requires the flexibility to bring together the appropriate employees in an organization in project teams, and the IT systems must support the efficient handling of processes (Schenk and Dietrich, 2018, p. 269).

However, if only the technological prerequisites of digitization or the modernization of the administration are discussed, this does not go far enough. Securing infrastructures, applications, and thus processes, in short, information security (Section 2.2), must also be considered in administrative digitization (Gulden, 2018, p. 138).

There are numerous approaches to organize and coordinate this, such as ITIL, COBIT, CMMI, etc., which *JOHANNSEN* and *GOEKEN* summarize in a suitable overview (Figure 11) (Johannsen and Goeken, 2011). These approaches are already established in large municipalities and their service providers. In medium-sized and tiny municipalities, such tools are only found in exceptional cases (Schenk and Dietrich, 2018, p. 270).

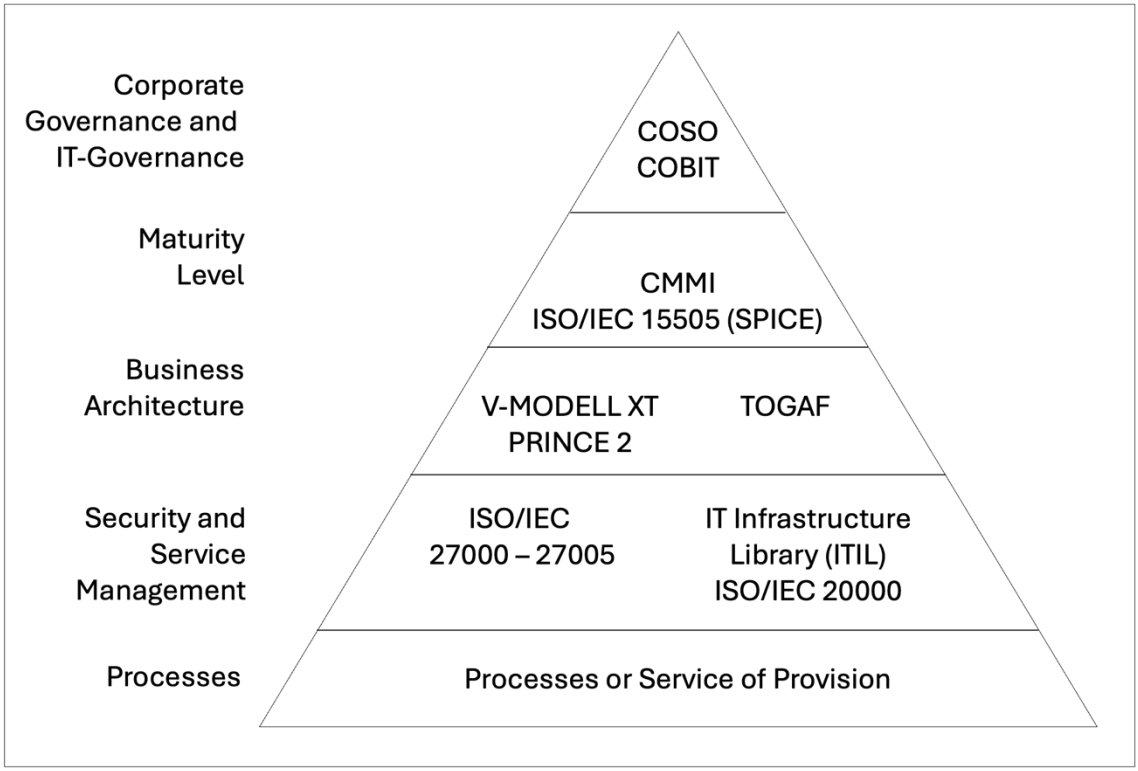

Figure 11: IT-Governance

2.1.4 Digitization and Information Security – A Challenge for Small Municipalities

As explained in Section 2.1, around 35% of local governments can be described as small to medium-sized local governments. On the one hand, these corporations are below the federal and state governments' levels and provide the population with specialist IT procedures to cover the core tasks of public administration. On the other hand, they perform many different tasks – with or without legal coercion – such as the sponsorship of kindergartens and schools to supply functions with electricity, gas and water.

The digitization efforts and the desire of citizens to interact more digitally with the administration pose significant challenges for small administrations. The list below provides an overview of the essential aspects:

- **Data protection and information security**: Administrations must protect sensitive data and preserve citizens' privacy. The increasing threat of cyberattacks requires constant adaptation of security measures (Markus and Meuche, 2022, p. 209; Rehbohm and Kalmbach, 2023).
- **Digitization of processes**: Moving to digital often requires significant investment in technology and employee training (Kremer, 2018, p. 205; Müller, 2018, p. 289). There are challenges in integrating new systems while maintaining existing, often outdated systems (Heuermann et al., 2018b, p. 300ff; Markus and Meuche, 2022, p. 20ff).
- **Interoperability**: Administrations need to ensure that their digital systems can communicate with each other to provide efficient information exchange. Interoperability issues can hinder the seamless integration of systems (Klenk et al., 2020, p. 31ff).
- **Lack of skilled workers**: The shortage of qualified IT security and digitization experts is a widespread challenge. Public administration competes heavily with the private sector for professional workers (Markus and Meuche, 2022, p. 3).
- **Citizen participation and acceptance**: The introduction of digital processes requires the approval and cooperation of citizens. There are challenges in involving the population in the process and ensuring that digital solutions meet their needs (Gulden, 2018, p. 138; von Lucke, 2021, p. 134).
- **Legal framework**: Compliance with legal regulations in data protection and IT security is a significant challenge. Legislation must often adapt to ever-changing technologies (Hanschke, 2020a, p. 8ff).

These challenges require a comprehensive and coordinated approach to ensure the success of digitalization projects in German administrations (Gulden, 2018, p. 142ff). At the same time, the increasing digitization of administrative processes also means a rising potential danger. To this end, appropriate security measures must be considered from the outset (Kremer, 2018, p. 201). Unfortunately, we are currently observing that the efficiently organized and previously well-functioning administrative apparatus is reaching its natural, historically evolved limits (Schwarzer, 2018, p. 489). This insight was already recorded in the first cyber security strategy of the German government in 2011. Cyber security is not a static, final goal but a "... the desired state of IT security, in which the risks from global cyberspace are reduced to an acceptable level" (von Salden and Schäfer, 2018, p. 532). The demand of *VON SALDEN* and *SCHÄFER* is obvious: The state must counteract the threat by organising the cyber security architecture accordingly to fulfil its protective mandate.

However, the legal framework for the municipalities is currently lacking. The NIS-2 Directive is a new edition of the obligation of the federal and state governments to establish a cyber security architecture. However, this does not directly address the local government. Against this background, cyber security tasks are assigned to "self-government" by those responsible for local governments (Rehbohm and Kalmbach, 2022, p. 339). It remains to be seen whether an expensive project to introduce an ISMS will be planned in the face of tight public budgets and a shortage of skilled workers.

The fact that information security also poses an existential challenge for municipalities is shown by the district of "Anhalt-Bitterfeld", which had to maintain a cyber disaster for months after an attack in the summer of 2021 (Lang, 2022, p. 27). Despite the establishment of federal and state information security agencies and increasing attacks, the issue is not receiving the necessary attention (Meuche, 2022, p. 100).

The reasons are varied: On the one hand, technical safeguarding of the systems requires investments, which are not made as long as those responsible do not see themselves affected (Grigat et al., 2020, p. 23), (Birk, 2021, p. 677). On the other hand, the risks lie to a considerable extent in the organization and in the knowledge and motivation of management and employees. Although public authorities now usually have information security officers, they are only active in an advisory capacity as staff units and do not have the authority to issue directives necessary for implementing measures. The leadership positions must enforce their advice, but they need the essential basic understanding to do so. This is especially true because information security must be considered in all strategic decisions (BSI, 2017, p. 35).

The question remains as to what degree of maturity the local government must meet digitization on the one hand and the associated challenges, such as information security and the needs of stakeholders, on the other.

An administration oriented towards the needs of the stakeholder groups with cross-functional processes first requires a changed legal framework and then a change in the structure, leadership, organizational culture, employee thinking, the orientation of training, and finally, the control system. The latter must focus much more strongly than is usual today on service and consulting, leadership and data quality and the associated security, and must be oriented towards the overarching goals. The maturity model of the Digital Administration Competence Center at Hof University of Applied Sciences addresses all of these aspects, although it is noticeable that no maturity level for "security" was determined in the study (Figure 12) (Henning et al., 2022, p. 6):

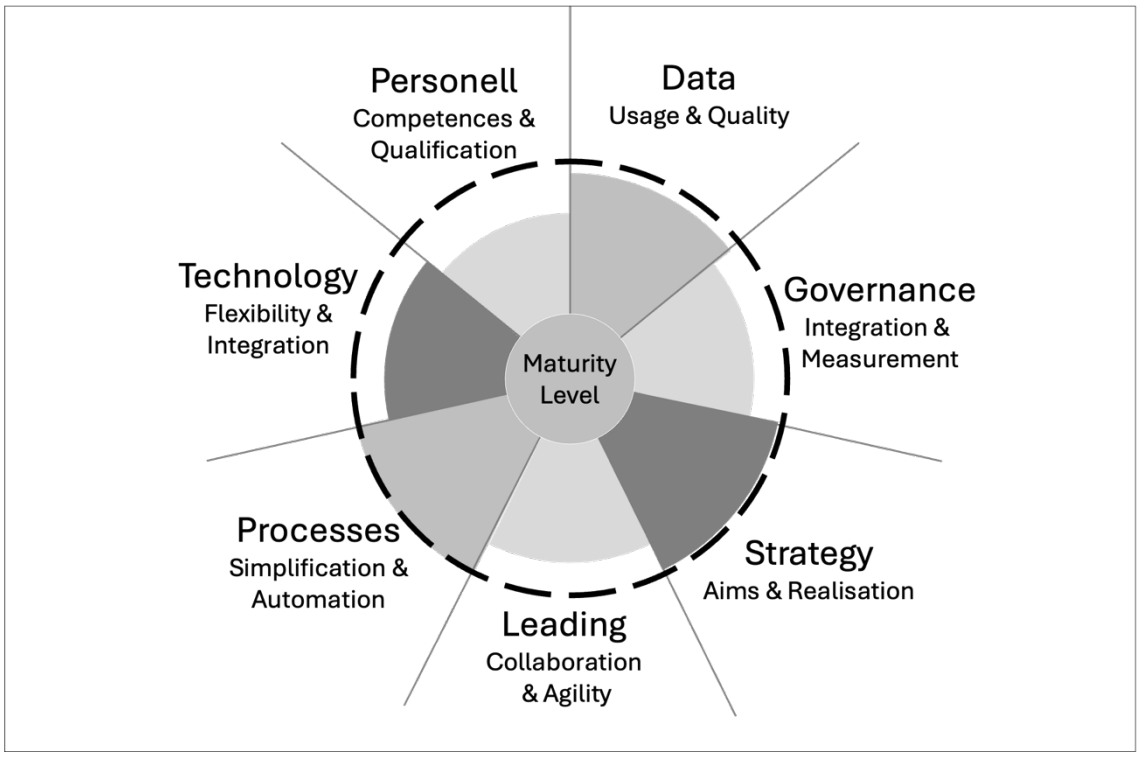

Figure 12: Maturity Model

However, the study makes it clear which aspects must be considered when developing a process model for establishing an ISMS.

In the federal system of the Federal Republic of Germany, the municipal level plays a central role in the perception of public administration because it represents the direct contact between citizens and companies for many matters. Although this proximity is given by the provision of services in the municipalities, there is little clarity in this area about the reasons for the timid digitization (Hornbostel et al., 2022, pp. 6, 29).

2.2 Information security as part of Cyber Security

2.2.1 The term Security

To define the family of terms information security or IT security, it is first necessary to understand the term security.

Safety can be understood as the absence or limitation of significant hazards. However, the term security offers a wide range of interpretations: (Freiling et al., 2014, p. 17)

- **Certainty** about the correctness of a statement, i.e. certainty in the sense of indubitability (doubtlessness, certainty)
- **Degree of trust** in the correctness of a statement, i.e. certainty in the sense of the certainty of the statement (confidence level)
- **Pledge or surety**, i.e. security in the sense of guaranteeing an equivalent value in the event of a loss (guarantee)

Even concerning the presence of hazards, the term security can have different meanings depending on the context of the application. The term security can refer to:

- The absence of dangers if damage cannot occur or can occur to a non-significant extent (ISO 27000)
- Adequate safety of hazards if, in the sense of limited, tolerable risk, significant cases of damage are only possible if the probability of occurrence is correspondingly low (IEC 61508)

2.2.2 Information security and IT security

This concept of security is often found in the relevant literature in conjunction with other terms, such as information security and functional security. *Abts* and *Mülder* understand **functional safety** as the safety of technology against system errors. These are mainly faults that occur due to software errors or external events. The definition of information security follows this. **Information security** aims to protect information, both electronically stored and in paper form. The term information security is often used synonymously with IT-security. **IT security** refers to a state in which risks and threats are reduced by appropriate measures (Abts and Mülder, 2017, p. 599; Hanschke, 2020a, p. 2). Information security always has something directly to do with individual personal behaviour and is not just the collection of technical measures. However, information security is also often associated with additional costs (Liedtke, 2022, p. 11)

2.2.3 Protection objectives

The German Federal Office for Information Security (BSI) defines information security analogously to the definition of *Abts* and *Mülder* but expands it to include essential protection goals (BSI, 2023, p. 3).

Similarly, the U.S. National Institute of Standards and Technology (NIST) defines information security. It includes protection goals in its definition: „*the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability*.“ (Paulsen and Byers, 2019, p. 94).

The international standard ISO 27000 is even shorter at this point. It defines information security as the „*preservation of confidentiality, integrity and availability of information*“ (*DIN ISO/IEC 27000*, 2016, p. 6) and thus focuses on the protection goals.

These three protection goals reflect precisely what the user expects as the secure use of data, namely that the IT system is available for use without manipulation and that data cannot be read or changed without authorization (Hanschke, 2020a, p. 52ff):

- information confidentiality: confidential information must be protected from unauthorized or unintentional disclosure
- data integrity: the data must be provided in full and unaltered
- availability: the user must have access to the services, functions of an IT system or even information at the required time

Figure 13: Security triangle (CIA)

The criticality of a business process determines the need for protection and, therefore, the level of information security to be achieved. The core elements of information security or protection objectives (CIA) must be identified, defined and considered individually depending on the environment and application (Liedtke, 2022, p. 19). Further protection goals can be regarded as if the analysis is extended to data protection aspects (Section 2.2.5).

2.2.4 Cyber Security

To achieve these goals, it is necessary to implement various organizational, but mainly technical security measures. These measures fall into different security areas, which can be summarized under the umbrella term cyber security (Li and Liu, 2021; Wollinger and Schulze, 2020).

Information security is, therefore, a part of cyber security (Pohlmann, 2022, p. 2). Cyber-security includes practical measures to protect information, networks and data against internal or external threats.

A definition or more detailed description of the sub-areas of cyber security is omitted in this thesis, as the sub-area of information of an organization is the focus of the study. Nevertheless, the following figure illustrates the distinction between information security and cyber security (Figure 14).

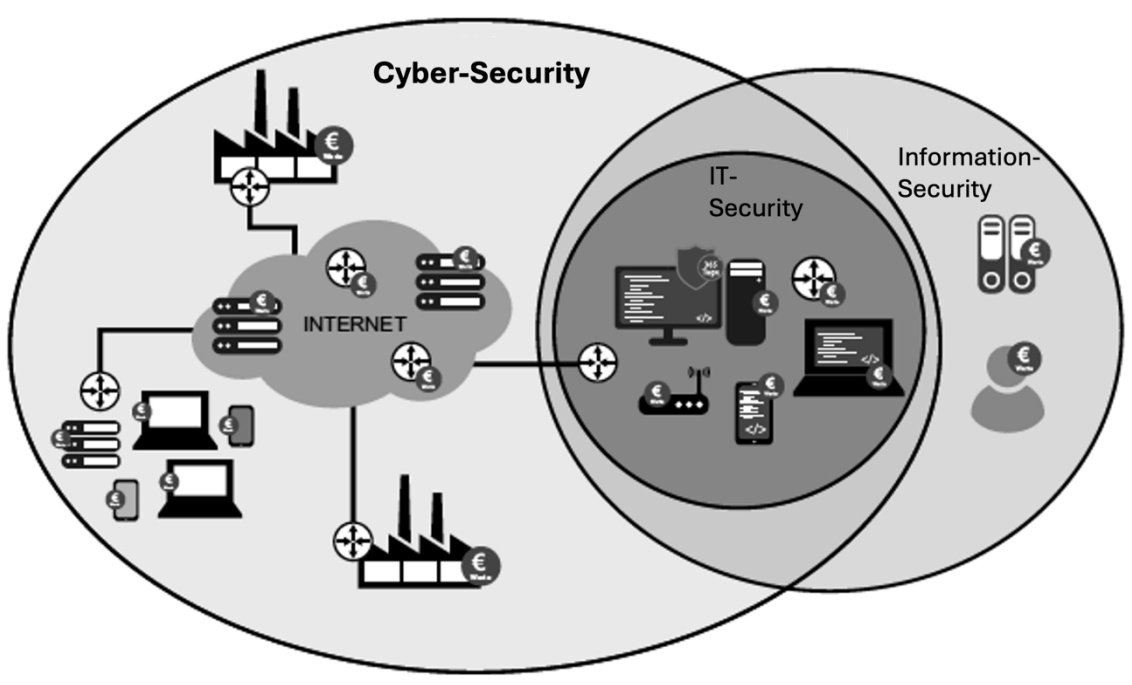

Figure 14: Cyber-Security

Source: (Liedtke, 2022, p. 15; Pohlmann, 2022, p. 5).

In the meantime, the term "cyber" is used inflationary in connection with other nouns in the literature (Jörgens, 2023, p. 6). Therefore, the term information security is mainly used in this thesis.

2.2.5 Data protection and data security

There are two significant differences between **information security** and **data protection**: On the one hand, information security requirements for most companies and institutions are based on independent decisions and are not primarily driven by regulations or laws. This means that these organizations subordinate themselves to specific guidelines that are out of their interest. These are usually also created by the organizations themselves. There is, therefore, no external influence. A notable exception is the operators of so-called critical infrastructures.

In contrast, external requirements have always controlled or determined data protection. With the entry into force of the General Data Protection Regulation (GDPR) on 24 May 2016, the requirements formulated apply to all organizations that work with personal data. This highlights the second significant difference in information security. While the scope of information security considers all information regardless of its content, data protection only applies to information with a personal reference (Jörgens, 2023, p. 5).

Therefore, data protection is inextricably linked to personal data protection (Lenhard, 2020, p. 3).

There are different definitions for the term data security:

SCHULTE and *SCHRÖDER* understand data security as an essential component of data protection. While data protection focuses only on personal data, data security knows no separation between personal and non-personal data. Data security should be understood less as a technical term and more as the result of legal considerations (Schulte and Schröder, 2011, p. 859).

Jörgens *FOLLOWS* this with his definition that "the term data security originates from data protection and refers to the technical protection of data, i.e. the fulfilment of protection goals" (Jörgens, 2023, p. 6).

Since data security pursues the same goals as information security, this thesis uses these two terms synonymously.

In addition to the three protection goals already listed in Section 2.2.3, the following other protection goals apply in the area of data security: (Liedtke, 2022, p. 20), (Rost and Pfitzmann, 2009, p. 354), (Petrlic et al., 2022, p. 10f)

- **Authorization**: Ensuring that people who wish to perform actions have the appropriate rights (role and authorization concept)
- **Authentizität**: Actions can only be performed by people who have authenticated or identified themselves accordingly.
- **Non-repudiation / Binding**: In particular, communication processes are recorded so that no falsification is possible, i.e. contingency can be guaranteed.
- **Controllability:** Data is not processed without the knowledge of the person responsible.
- **Transparenz:** How personal data is processed is understandable to third parties.
- **Intervenability**: The affected subject can intervene against processing, i.e. edits can be revised.
- **Disassociability**: Different data is stored so that they cannot be linked to each other.

The fulfilment of these protection objectives is in the interest of every organisation, although the protection objectives can also be derived from different laws. Information security management systems provide essential building blocks for fulfilling these protection goals.

2.3 Information Security Management

Establishing an ISMS suitable for the organization forms the basis for documenting and coordinating security processes in a structured and transparent manner (Böhmer et al., 2017). In medium-sized to large administrations, the BSI baseline protection or the ISO 27001 standard have been established recently. Both ISMS standards are suitable for analysing, structuring and optimizing the complex security standards in public authorities. These two standards are generally unsuitable for small organizations due to their scope and complexity. Nevertheless, these two standards will be discussed here and briefly described before a procedure model for small administrations is developed and evaluated.

2.3.1 ISO/IEC 27001

The ISO/IEC standard has established itself internationally as the standard for implementing information security in companies and administrations. It is based on the British standard BS 7799-2 and was first published as an ISO standard by ISO and IEC in 2005 and is part of the ISO/IEC 2700X family of standards. The latest version of this standard was published in October 2022 and defines the international standard for an information security management system (ISMS) (*DIN ISO/IEC 27000*, 2016; *DIN ISO/IEC 27001*, 2018)

ISO/IEC 27001 contains requirements and measures for establishing, operating and continuously improving an ISMS. It is important to note that the ISMS must be adapted to the organisation's specific characteristics (Hanschke, 2020a, p. 10). Furthermore, the standard family includes some guidelines on special topics such as risk analysis or preparation for an audit. The figure below provides an overview of the individual standards and then explains the content: (Figure 15)

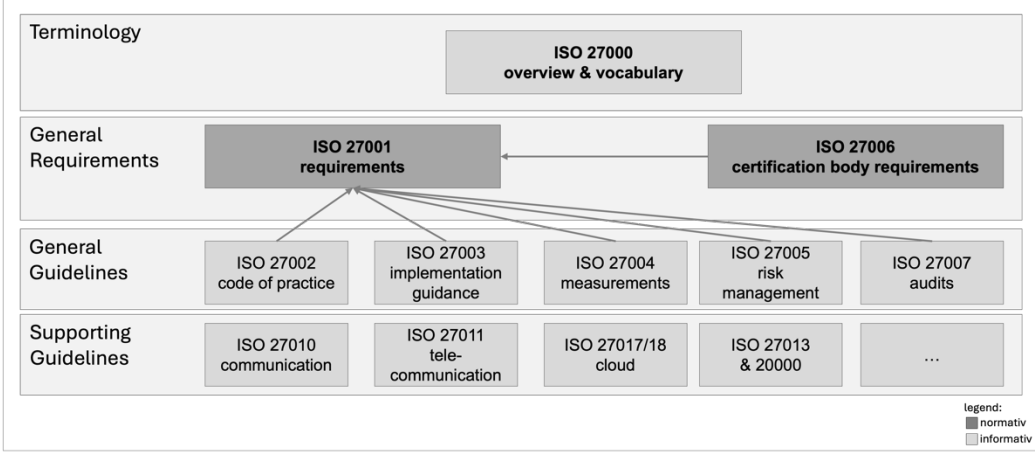

Figure 15: ISO/IEC 2700X Norm-Family

The individual standards have different objectives and areas of application, which are briefly summarized as follows (Böhmer et al., 2017, p. 24ff; Kersten et al., 2013, p. 13):

- **ISO/IEC 27000** contains the basic principles, concepts, terms and definitions for ISMS and provides an overview of information security management systems (ISMS) and the interrelationships between the various standards in the ISO-2700X family.
- **ISO/IEC 27001** is the central and only certifiable standard in the ISO 27001 family of standards. The standard consists of 10 sections, and Annex A. Sections 1-3 are general recommendations for the ISMS's introduction, operation, and improvement. Sections 4-10 are mandatory, meaning all the requirements therein must be implemented.
- **ISO/IEC 27002** is the code of practice and contains generally formulated requirements.
- **ISO/IEC 27003** guides how to implement the ISMS.
- **ISO/IEC 27004** is a guideline for the development and execution of measurements that can be used to measure the effectiveness of the ISMS.
- **ISO/IEC 27005** describes the process-oriented risk management approach.
- **ISO/IEC 27006** specifies requirements for the accreditation of certification bodies and guides the ISMS certification process.
- **ISO/IEC 27010** defines the exchange of security information, e.g. in critical infrastructures.
- **ISO/IEC 27011** provides guidance for ISMS in the telecommunications sector.
- **ISO/IEC 27013** serves as a guideline for integrating an ISMS according to ISO/IEC 27001 and IT service management according to ISO/IEC 20000-1.
- **ISO/IEC 27017** contains extensions for the implementation of cloud services.
- **ISO/IEC 27018** describes implementation instructions for securely processing personal data.

The standard body of ISI/IEC 27001 has the following structure (Figure 16). With the help of this structure, the individual chapters can be run through a PDCA cycle.

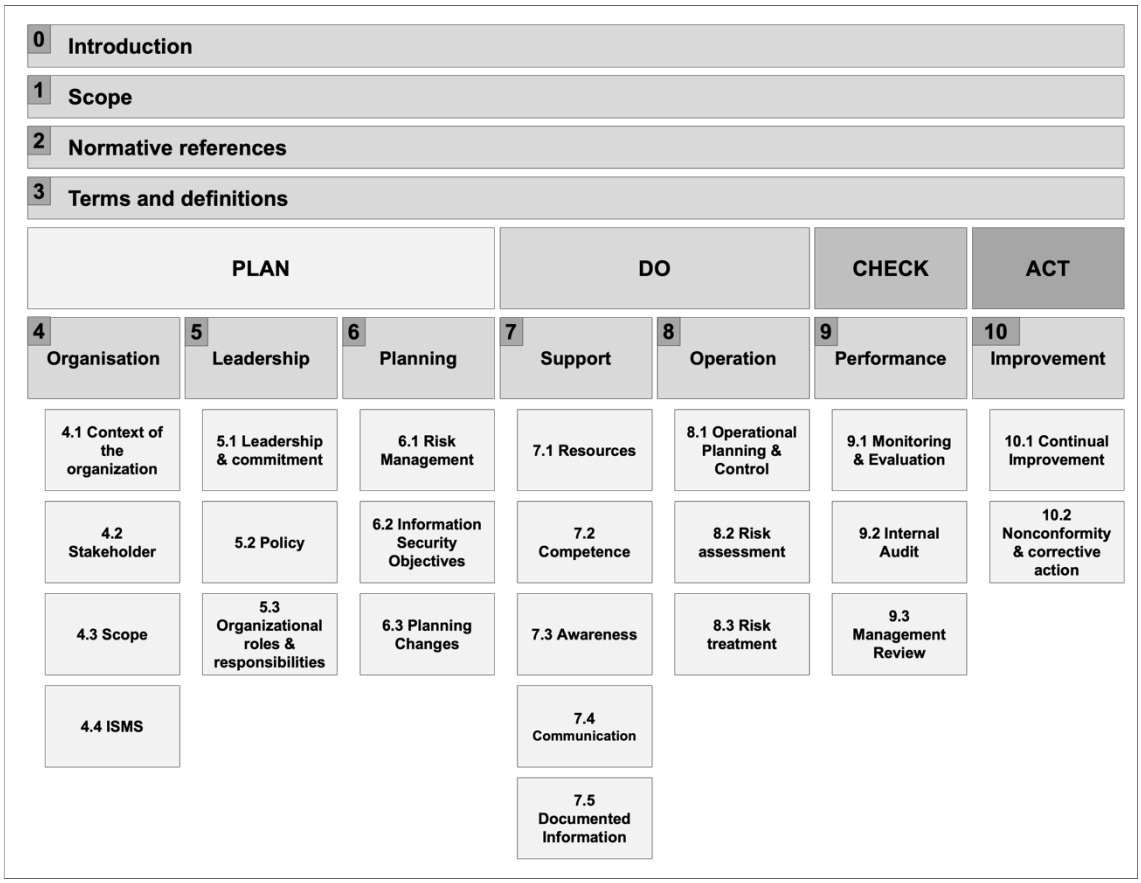

Figure 16: ISO/IEC 27001

The individual chapters contain the requirements that the affected organization must establish. A distinction can be made between planning and operational tasks. The dispositive measures are to be fulfilled by the organizational management, and the operational measures by the respective responsible organizational units. The guidelines of the standard family supplement the abstract formulations and are to be used to aid in implementing the ISMS.

Annex A of ISO/IEC 27001 contains the 93 measures that are divided into the following sub-areas

- Organizational controls
- People controls
- Physical controls
- Technical controls

but only contain an abstract overview of the implementation measures. The Code of Practice provides a detailed description of the requirements. These requirements must be implemented for the organization's assets.

The aim of setting up an ISMS according to ISO/IEC 27001 is to subject an organization's assets to a risk assessment, taking into account the stakeholders' requirements and establishing appropriate security measures for risk treatment.

2.3.2 IT Baseline Protection

On the other hand, there is the IT baseline protection of the Federal Office for Information Security (BSI). It is understood as a defacto standard for information security and has a national character. IT baseline protection is a framework that supports organizations in ensuring their information security. It offers a structured approach for setting up an ISMS and is particularly common in Germany among medium- to large administrations ("BSI-Standard 200-1," 2024; "BSI-Standard 200-2: IT-Grundschutz Methodik," 2024; "BSI-Standard 200-3: Risikomanagement," 2024; "BSI-Standard 200-4: Business Continuity Management," 2024).

IT baseline protection is based on the baseline protection manual, which provides a comprehensive collection of measures and recommendations for information security. The handbook consists of various modules that focus on different aspects of information security. These include organizational, personnel, infrastructural and technical measures (Figure 17).

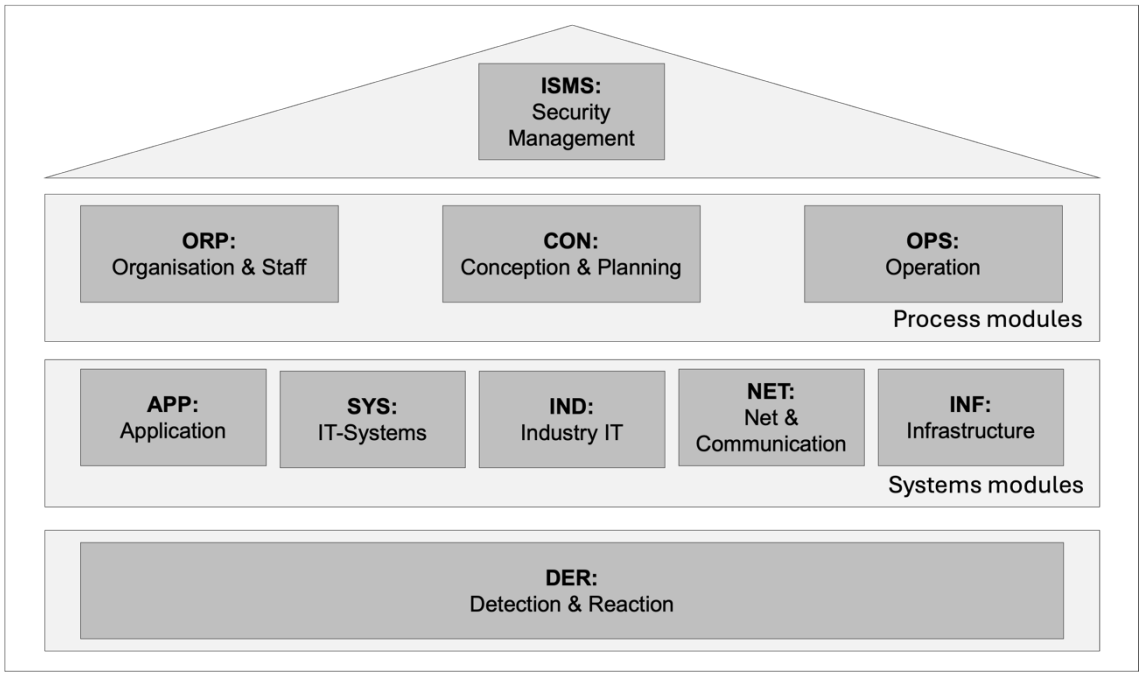

Figure 17: Layer and modules of IT basic protection

In addition to the basic protection manual, the user is supported by four BSI standards. These BSI standards contain recommendations on methods, processes and procedures, as well as procedures and measures for various aspects of information security ("BSI-Standards," 2024):

- **BSI-200-1** defines general requirements for an information security management system. It is widely compatible with the ISO 27001 standard and considers the recommendations of other ISO standards, e.g., ISO 27002.
- **BSI-200-2** forms the basis of the BSI methodology for setting up an ISMS.

- **BSI-200-3** bundles all risk-related work steps in the implementation of IT baseline protection.
- **BSI-200-4** provides practical guidance on how to set up and establish a Business Continuity Management System (BCM) in the organization.

The development of an ISMS with IT baseline protection takes place in several steps:

1. **Inventory and definition of protection needs:**
   - Identification of information and IT systems: Determine which information and systems need to be protected.
   - Determination of protection requirements: categorisation of information and systems according to confidentiality, integrity and availability.
2. **Systematic risk analysis:**
   - Identification of threats and vulnerabilities: Analysing the potential risks to the identified information and systems.
   - Assessment of the risks: Estimating the probability of occurrence and potential damage impact.
   - Definition of protection targets: Defining objectives to reduce the risks.
3. **Selection of measures and implementation:**
   - Selection of safety measures: Suitable measures are selected based on the fundamental protection manual.
   - Implementation of the measures: Integrating the selected measures into the existing IT infrastructure.
4. **Documentation and verification:**
   - Documentation of the measures taken and protective mechanisms.
   - Regular reviews and updates: The ISMS is continuously monitored and adjusted as required.
5. **Certification according to ISO/IEC 27001:**
   - Certification option according to IT-Grundschutz by the BSI.
   - Optional, but often desired: ISO/IEC 27001 certification makes it possible to review and confirm the implemented ISMS following international standards.

The BSI's IT baseline protection provides practical guidance for organisations to establish and improve their information security. By applying this framework, organisations can better protect their IT infrastructure and arm themselves against current threats.

2.3.3 Comparison of ISO/IEC vs. IT Baseline Protection vs. CISIS12

The process models presented here have different advantages and disadvantages. The following table (Table 4) extracts various criteria for which the individual process models can be differentiated (Kersten et al., 2013, p. 16ff; Moses and Rehbohm, 2022a, p. 67). At the same time, this table compares the process model developed in this work with the two described here.

Table 4: Comparison of process models

	Information Security Approaches		
Criterion	**CISIS12**	**ISO 27001**	**IT-Basic protection (BSI)**
Publication body	IT Security Clusters e.V.	International Standardization Organization (ISO)	Federal Office for Information Security (BSI)
Guidance	Yes, 30 pages	Yes, 30 pages	No,4 BSI-Standard Documents, approx. 250 pages
Target area	DACH-Region	international	national
Target group / Size	small to medium	small to large	small to large
Complexity	high	high	high
Structure and scope of the catalogue	procedural model, 86 modules and 865 measures	93 Controls	113 modules with 1,836 measures
Risk analysis	Yes, mandatory	Yes, mandatory	Supplementary for high protection requirements
Implementation	Goal-oriented and easy-to-implement process model with concrete measures	No process model, generally formulated measures	An abstractly formulated process model, implementation of measures based on the catalogue of measures
Certification Opportunity	Yes, independent accredited certification bodies	Yes, independent accredited certification bodies	Yes, BSI Certification
Tool support	Yes	Yes	Yes
Time required for implementation	< 12 months	> 12 months	> 12 months
External costs	depending on the certification program and size of the organization: 10,000-30,000€	depending on the certification program and size of the organization: 30,000-50,000€	depending on the certification program and size of the organization: 30,000-100,000€
Effort	Introduction of an ISMS with appropriate risk management and security measures derived from it	Introduction of an ISMS with appropriate risk management and security measures derived from it	High formal effort for modelling and protection needs analysis
Procedural Model	Yes	No	Yes, but very complex

2.4 Management Concept

The terms management, organisational management or corporate management can be interpreted differently. Management and corporate management are often used synonymously. In this context, all factual and thematic tasks associated with general questions of corporate management are addressed. In addition, the term management can also be extended to other organisations (in the institutional sense), e.g. administrations. The term management (Figure 18) is usually differentiated into functional and institutional management concept (Bea and Göbel, 2019, p. 25ff; Becker and Fallgatter, 2005, p. 14; Schreyögg and Geiger, 2016, p. 5ff; Vahs, 2015, p. 16ff).

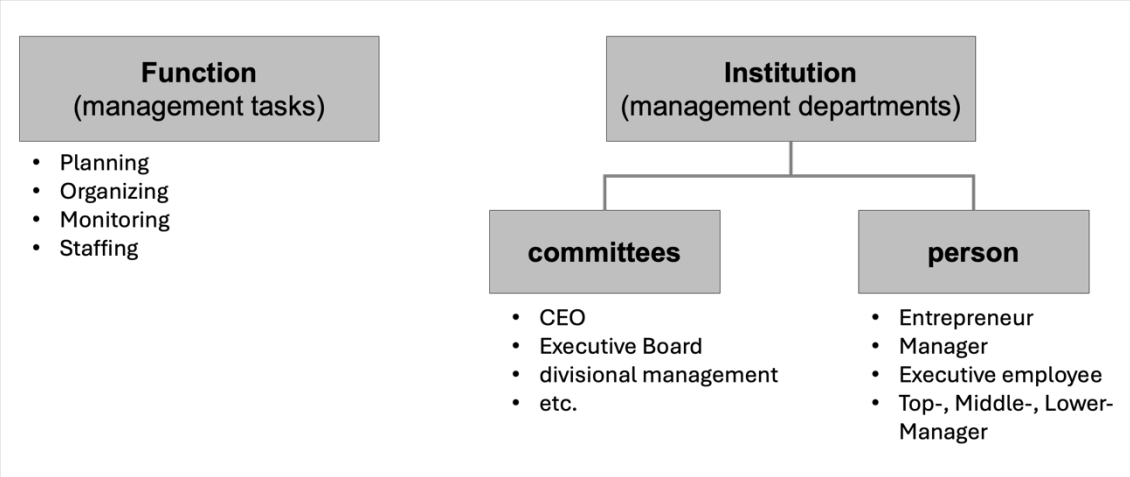

Figure 18: Differentiation of the concept of management.

The activity- or process-orientated (functional) term is to be understood as a goal-orientated process for structuring wholes, which is carried out by certain persons (role holders). Within this process, action orders are designed, and a binding order is given to the organisation's members by the management level (Grunwald, 2022, p. 14ff). While the **functional** term is aimed at the individual management tasks (planning, organisation, control and personnel) of the persons entrusted with management, the **institutional** management term covers the persons or committees and their role holders.

2.4.1 Management as an Institution

The institutional management concept views the organisation in its entirety as an institution. An institution is a system of norms and rules accepted as binding by the organisation's members and has specific stability (Göbel, 2021, p. 15ff). At the core of this definition is, therefore, not the process of organising, nor the formal structure of the company or administration, but rather the entire social structure with formal and informal elements (Schreyögg and Geiger, 2016, p. 9).

BECKER and *FALLGATTER* define "management as an institution" as the carriers of the management processes, i.e. the centres of decision-making (Becker and Fallgatter, 2005,

p. 15). From this institutional perspective, the focus is on these units' composition, roles, and functioning (managerial role approach).

People who fulfil such roles are referred to as executives or managers. At the same time, committees are formed to achieve specific management tasks, such as executive management. The committees' personnel organisation ranges from one person to several people. These institutional units must fulfil management tasks, whereby their decision-making powers and authority to issue instructions are not linked to the person in charge but to their formal position in the organisation. They work in a division of labour and are equipped with different competencies (Vahs, 2015, p. 49ff).

Depending on the hierarchical level and the positioning of the individuals or committees, the internal power hierarchy can be categorised into top, middle and lower management. The hierarchical categorisation addresses different types of tasks and areas of responsibility (Figure 19). While top management (company management) is responsible for developing principles, objectives and strategies, middle management is primarily responsible for implementation and operational management. Lower management coordinates the operational realisation of tasks at the interface to the execution level (Becker and Fallgatter, 2005, p. 16).

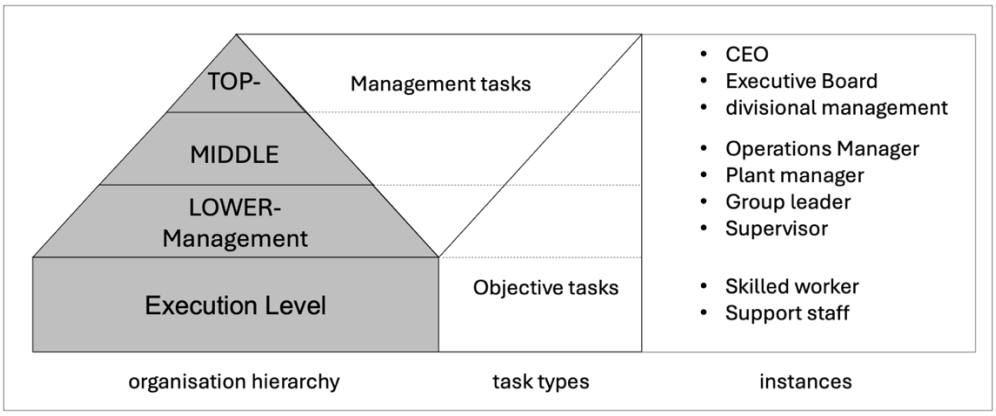

Figure 19: Hierarchical division of labour

2.4.2 Management functions

The functional management concept contributes, in particular, to the understanding of corporate management, management systems and processes, and strategic management. Essentially, the functional management concept addresses the tasks that must be fulfilled in the system and process of managing a company based on a division of labour (managerial functions approach). The management tasks to be fulfilled by managers can be diverse and heterogeneous in terms of content. However, they are similar if the core tasks are handled in management. Regardless of the hierarchical level, these rather general and homogeneous core tasks are known as management functions. They relate to the services to be provided by the management institution that are necessary as part of the management process to maintain the management system and achieve the company's

objectives. These management tasks include the factual activities of decision-making (analysis, planning and decision-making) and implementation (initiating implementation, management and control) as well as personnel-related tasks of personnel management (Schreyögg and Geiger, 2016, p. 5).

KOONTZ/O'DONNEL break down the complex "management functions" into typical subtasks (Koontz and O'Donnel, 1976). This provides an accepted framework of essential functions (Figure 20).

Figure 20: Management functions of Koontz and O'Donnell

The management functions describe tasks that are to be performed by managers. They can only be fulfilled if the necessary requirements are met. *KATZ* (Katz, 2009, pp. 90–102) first identified three critical competencies of a manager in 1974 and defined the concept of skills as follows: *„As used here, a skill implies an ability which can be developed, not necessarily inborn, and which is manifested in performance, not merely in potential. So the principal criterion of skillfulness must be effective action under varying conditions."*

This definition of skills is in line with our current understanding of competencies. Today, these three key areas (Figure 21) can be interpreted as follows (Berthel and Becker, 2003, p. 265; Melzer et al., 2019, p. 17ff; Moser, 2018, p. 11ff; Steinmann and Schreyögg, 2000, p. 20):

- **Professional competence** (disposition to act cognitively self-organised) relates to detailed knowledge and the technical application of methods and procedures in task-related task fulfilment. It is essential at the lower management level.
- **Social competence** (disposition to act in a communicative and cooperative self-organised manner) refers to the ability to work efficiently with other people in personal task fulfilment. This is important for group tasks, supervisor-employee relationships, and other interpersonal interactions.
- **Methodological competence** (disposition to act instrumentally self-organised) emphasises problem awareness, a holistic view, the ability to recognise

interdependencies between company divisions or processes, know-how, and independent problem-solving behaviour such as critical, analytical and networked thinking. Methodological expertise is more important at higher management levels.

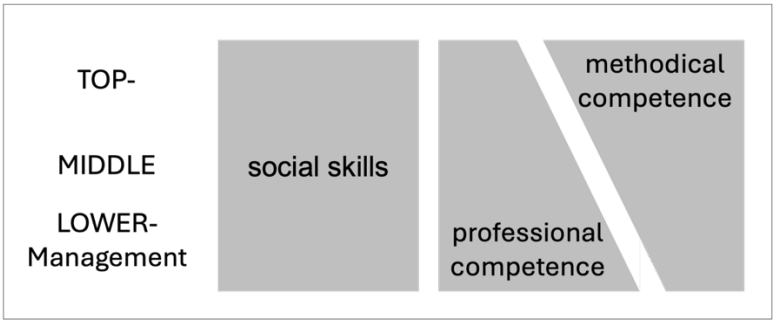

Figure 21: Types of Competencies

In recent years, various authors have mentioned another competence, namely the so-called "personal competence". Personal competence subsumes resilience, flexibility, and willingness to learn, perform and self-develop. However, this will not be considered further in this paper.

2.4.3 Management Process

The management functions are not organised separately but in a specific order and sequence. In the management process, the functions are viewed as dynamic phases, ideally as a sequence of tasks that follow one another (Steinmann and Schreyögg, 2000, p. 11). In practice, corresponding feedback processes ensure that the overall process is made more flexible in terms of content and time, which means that several functions must be taken into account simultaneously when designing it.

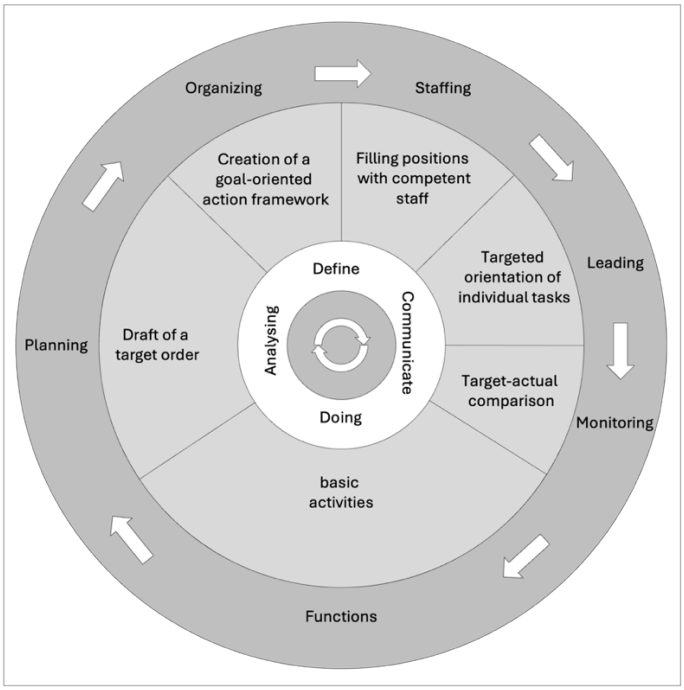

Figure 22: Cycle of Management functions

2.4.4 Managerial Role and Behaviour

The management functions do not describe the actual behaviour of managers but merely structure it. *MINTZBERG* categorises the behaviour of managers according to ten observed manager roles and divides these in turn into three activity groups (Table 5).

Table 5: Management Roles

	Interpersonal Relationships	Informational	Decision
Role	figurehead	monitor	entrepreneur
	leader role	disseminator	disturbance-handler
	liaison role	spokesman	resource allocator
			negotiator

These role descriptions and the behaviour of the respective person are essential for the present work and will be used later. With this in mind, the individual roles are briefly described based on *MINTZBERG* and *KUMAR* ((Kumar, 2015, p. 13f; Mintzberg, 1980).

- **The interpersonal roles** link all managerial work together.
  - **Figurehead Role**: The manager represents the organization in all matters or formality. The top-level manager represents the company legally and socially to those outside the organization. The supervisor represents the work group to higher management and higher management to the workgroup.
  - **Liaison Role**: The manager interacts with peers and people outside the organization. The top-level manager uses the liaison role to gain favours and information, while the supervisor uses it to maintain the routine workflow.
  - **The Leader's Role**: It defines the relationships between the manager and the employees.
- **The informational Roles** ensure that information is provided.
  - **Monitor Role:** The manager receives and collects information about the operations of an enterprise.
  - **Disseminator Role:** The manager transmits particular information into the organization. The top-level manager receives and sends more information from the people outside the organization than the supervisor.
  - **Spokesman Role:** The manager disseminates the organisation's information into its environment. Thus, the top-level manager is seen as an industry expert, while the supervisor is seen as a unit or department expert.
- **The decisional roles** make significant use of intelligence and have four decisional roles.
  - **Entrepreneur Role:** The manager initiates change and new projects, identifies new ideas, and delegates idea responsibility to others.

- **Disturbance-Handler:** The manager deals with threats to the organization. The managers take corrective action during disputes or crises to resolve conflicts among subordinates.
- **Resource-Allocator Role:** The manager decides who gets resources, schedules and budgets, sets priorities, and chooses where the organization will apply its efforts.
- **Negotiator Role:** The manager negotiates on behalf of the organization. The top-level manager makes the decisions about the organisation as a whole, while the supervisor makes decisions about their particular work unit.

2.5 Organisational Behaviour

2.5.1 Ability, Willingness and Consequence

A view that categorises competencies as either present or absent does not adequately reflect the company's reality. Competences are not an "all-or-nothing" phenomenon but are developed gradually, whereby the degree is fundamentally changeable (Krumm et al., 2012, p. 6).

If a person has the necessary competencies to cope with a complex situation, this can be referred to in the broadest sense as the ability to act (ability). This does not necessarily mean that the person translates these competencies into performance in an operational context. At the same time, inadequate performance does not necessarily imply a lack of competencies (Krumm et al., 2012, p. 5).

The individual's willingness to act is, therefore essential to generate a solution-orientated performance in addition to the determinant of ability (Berthel and Becker, 2003, p. 38).

For a project for the sustainable development of an ISMS, this means that the project manager should ask himself the following questions:

- How does motivation arise?
- What determinants influence the motivation and experience of employees?
- What framework conditions must be in place for a project to be successful?

The ability, willingness determinant concept (AWC) provides a good overview of the factors that motivate people to do something (Figure 23) (Berthel and Becker, 2003, p. 39).

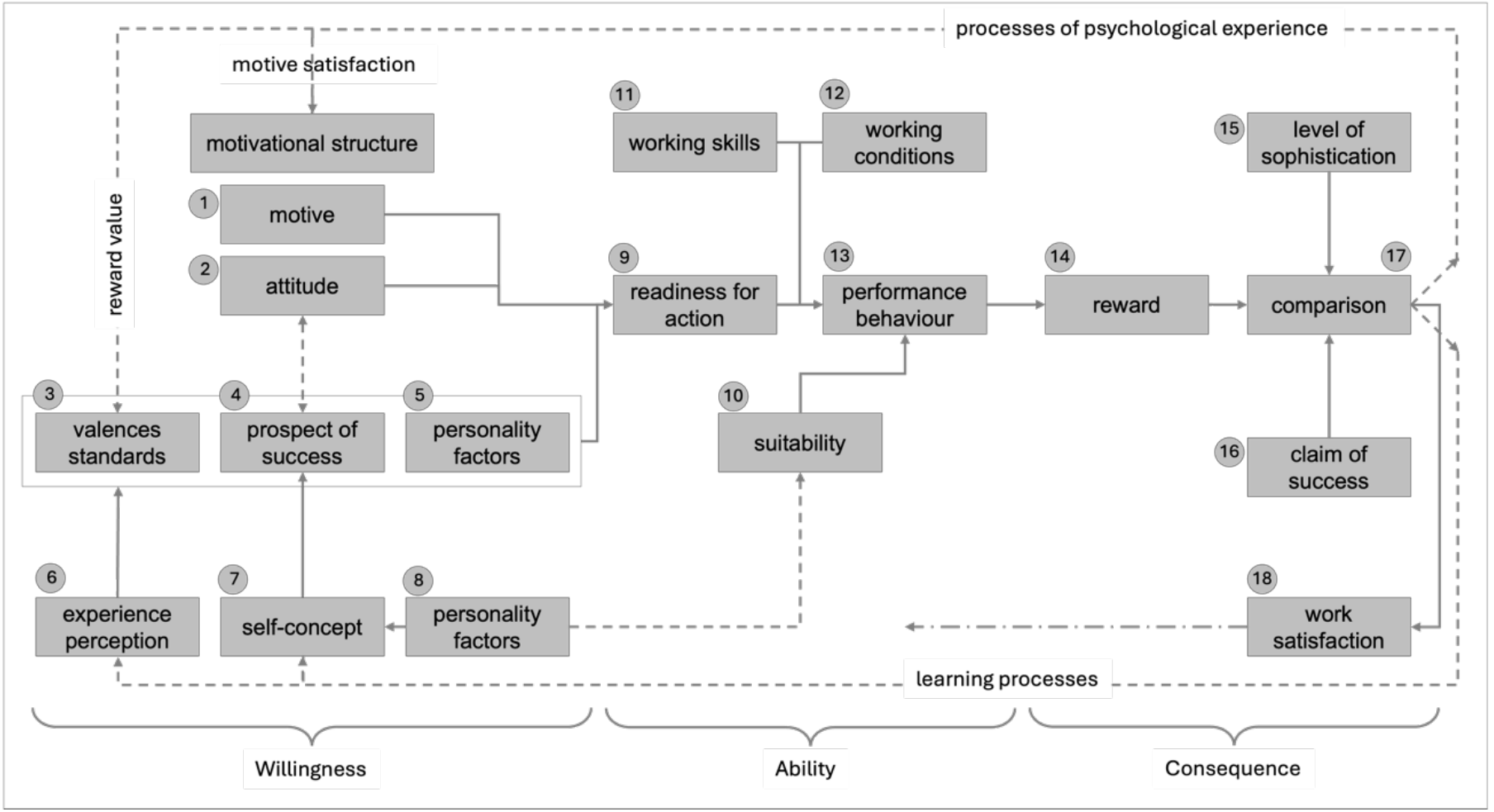

Figure 23: Ability-Willing-Consequences-Concept

The AWC consists of 3 components, namely the determinants of **Ability**, **Willingness** and **Consequences**.

Within the determinants of willingness, three essential building blocks work together.

Firstly, the employee's accumulated "experience", i.e. his (6) experiences/perceptions, his (7) self-concept and his (8) personality factors must be taken into account. The second building block, "motive structure", is indirectly influenced by these experiences. The (1) motives thus represent people's willingness to behave, which is triggered by specific incentives and influenced by (2) attitudes, which generally have a lasting character and result from experience. Furthermore, the valences and expectations of employees have a particular impact on the motive structure. A (3) valence is a person's positive or negative attitude towards the desired results or the adherence to specific rules (norms). On the other hand, (4)(5) expectations as a cognitive construct express the subjective probability calculation of a person in relation to the occurrence of one or more events. With expectations in particular, a distinction must be made between (4) effort expectation - the subjective probability that one's performance depends directly on individual effort and can also be achieved - and (5) consequence expectation - the subjective likelihood that individual goal achievement depends on one's performance and that the expected consequence will materialise.

All expectancy-valence approaches assume that the strength of a person's behavioural tendency depends on the individual level of expectation and the valence (attractiveness) of a situation for that person and the expected consequences. If the three components described above positively affect the employee, this results in (9) commitment.

Three factors characterise the determinant of ability. On the one hand, there is the (10) aptitude of an employee, i.e., the personal qualification characteristics, and (11) work knowledge, a kind of specialist knowledge that fulfils the task optimally. On the other hand, the (12) working conditions are factors that have a positive or negative influence on the (13) performance behaviour of employees or the organisation and also have a motivating effect at the same time (Berthel and Becker, 2003, p. 56ff; Wahl, 2013, p. 17).

The determinant of the consequences is primarily determined by the (14) reward for performance behaviour. The (15) aspiration level represents the level of a person's expectation or objective, and the (16) attribution or attribution of causes manifest themselves in (18) job satisfaction after a corresponding (17) comparison. In addition to these partly measurable factors, the AWC is determined by experience and the resulting insights (i.e. learning). The successful solution of a difficult task, the subsequent satisfaction experienced (psychological expertise), and the reward received can positively influence motivation for future opportunities. The ability and willingness to act can be promoted by company incentive systems such as performance-related remuneration systems or the expansion of responsibility and autonomy, and they are the subject of classic personnel development.

Comelli and *Rosenstiel* point out that the approach of the Ability-Willing-Consequences-Concept with its three determinants falls short and extend this model to include the determinant "**may**". That means the permission "**may**" is required for the action. It can be explicitly given or implicitly presented as a matter of course (Comelli and Rosenstiel, 2011, p. 3). This component, in particular, is primarily determined by the type of organisation (sector), the motivation of the management level, the organisational structure and the degree of managerial hierarchy. The more hierarchical an organisation is, the less autonomy individuals will likely have to apply their skills.

In the sense of an observable action or performance, performance is a product of situation-specific competencies and their activation as a result of certain incentive systems, flanked by corporate structures that grant a high degree of autonomy. Performance can only be achieved if personnel and organisational development are integrated into an overall concept (Berthel and Becker, 2003, p. 56ff).

2.5.2 Group dynamic effects

Hardly any critical decision, whether in politics, family or at work, is made by a single person. Interestingly, socio-psychological research shows that groups often make blatantly wrong decisions: group decisions are not automatically better than individual decisions. The literature distinguishes between the group dynamic effects described below.

2.5.2.1 Hidden-Profile-Effect

Groups mainly discuss shared or opinion-confirming arguments, whereas contrary opinions are ignored. The group, therefore, primarily talks about what everyone already knows. This phenomenon is known in psychology as the **hidden profile effect** (Berthel and Becker, 2003, p. 420; Stasser and Titus, 1987). The specialised knowledge of the individual group members is ignored, and the focus is only on the knowledge that confirms opinions. This results in significantly less overall knowledge, which also strongly influences the quality of decisions.

2.5.2.2 Risky-Shift-Phenomenon

Another phenomenon is that group decisions are often more extreme than individual decisions, i.e., the group's risk appetite is higher than that of the individual. Initially, it was assumed that the extreme opinions of individual group members would be "averaged out" in joint decision-making. However, contrary to this assumption, group polarization often occurs, so the group tends to make a riskier decision. *Stoner* calls this phenomenon „**Risky-Shift-Phenomenon**“ (Stoner, 1961).

2.5.2.3 Social Loafing

In a group, it is difficult to measure a person's individual performance or contribution. Due to this fact, the phenomenon often occurs in groups, and the individual person further reduces his contribution. This phenomenon is referred to in the literature as "social loafing"

(Latané et al., 1979), whereby the loss of motivation increases with the size of the group (Karau and Williams, 1993).

2.5.2.4 Distribution and Diffusion of Responsibility

For all three phenomena in the context of group dynamic decision-making processes, the following explanations for the behaviour of group members are conceivable:

- **The distribution of responsibility** is the complete transfer of duties, competencies and thus responsibility to another person, whereby the actual controller feels little or no responsibility (Bartling and Fischbacher, 2012, p. 70).
- **Diffusion of responsibility** describes the phenomenon that a problem or necessity that needs to be solved or completed decreases the more people are involved, despite having sufficient knowledge, employees and attention, and the greater the number of people involved, the lower the individual's sense of responsibility for completing the task (Symmank and Hoffmann, 2017, p. 957).

Both phenomena are frequently encountered in the research domain. In particular, the diffusion of responsibility, according to the principle: NIMBY: „Not in my Backyard" or „The art of distributing work so that none will be left for yourself".

PART B – PUBLICATIONS AND RESEARCH CONTRIBUTIONS

You never fail until you stop trying.

Albert Einstein

Part B provides a summary of the research contributions. At the same time, an overview of the research methods used to create the individual contributions. Furthermore, the research questions answered by the contributions are assigned to the respective contributions. Subsequently, the publications are linked to the phases of the DSR process and then printed in their entirety.

3 Published Research on ISMS in Public Sector Organisations

In order to collect the relevant literature on the status quo of information security in the public sector and especially in local government, a structured literature analysis based on *WEBSTER* and *WATSON* (Watson and Webster, 2020) was carried out. The guiding research question was "In the context of information security management, what scientific work on information management systems for public sector organisations and on inhibiting factors for implementing them has been published?". Based on this research question, we identified the following keywords as relevant for the search: "cybersecurity, public sector, information security, inhibiting factor, hindering factor, obstacles". An initial on Google Scholar resulted in relevant papers from different scientific disciplines, such as business administration, administrative sciences, or computer science. Thus, we selected different, widely used electronic literature databases to reflect this variety: SSOAR (administrative sciences), EBSCO Econ Lit and WISO (public service), as well as Scopus (computer science, information systems and many other disciplines). In the preparation phase for the literature analysis, we also used German translations of the search terms to investigate whether ISMS implementation problems in small public sector organisations are primarily a phenomenon in the German public sector. However, it turned out that (a) the very few significant results in the German language were also linked to publications in the English language, and (b) publications from many other countries indicated the same ISMS problems. Thus, we continued with the English terms only.

As the introduction of GDPR in the EU in 2016 significantly affected the ISMS requirements, we decided to conduct a search period from 2016 to today. The search in the databases mentioned above for this period returned 703 unique articles. Articles only addressing technological issues of information security were excluded, which reduced the number of hits to 378. In the next step, articles irrelevant to the public sector were removed, leaving 165 articles. After assessing their relevance based on content, quality and citation frequency, **92 articles** were filtered out and included in further analysis. The results of the search queries are summarised as follows (Table 6):

Table 6: Result of Literature Review

search string join with AND	literature-database	hits	relevant
isms, success, factor	Scopus	269	26
isms, success-factor		172	17
isms, hindering, factor		16	4
cybersecurity, hindering, factor		6	1
cyber, security, hindering, factor		10	2
cybersecurity, municipal		20	8
information, security,		412	23

municipal			
information, security, success-factors, isms		21	9
isms, success, factor	EBSCO EconLit	8	0
isms, success-factor		4	0
isms, hindering, factor		0	
Cybersecurity		151	5
information, municipal		1	1
information, security, municipal		20	1
information, security, management, system		28	0
Cybersecurity	SSOAR	37	2
security, municipal	WISO	137	1
isms		4	1
information security		24	1

A literature review concerning the country of publication shows that significant research is taking place in the EU and the USA. The following table (Table 7) briefly summarises the research locations and the priorities. The main research areas relate to critical infrastructures, research into obstacles and success factors, overarching strategies, and technical and organisational measures. The subsequent literature review highlights a gap in terms of research that aims to develop and present a management system suitable for public administration. In particular, no publications were identified that focus on the demands of small public sector organisations.

Table 7: Research location and research fields

research location	amount	research field
EU (Bulgaria, Croatia Germany, Greece, Ireland Netherlands, Norway, Poland, Sweden, Turkey, UK, Ukraine)	17	security in public sector organisations, critical infrastructures, risk analysis, national strategies, maturity and procedural models, organisational success factor, modern cybersecurity threats, hindering / success factors, awareness / marketing, digital sovereignty, technical measures, status quo of security management systems, budgeting
USA	12	security in public sector organisations, national strategies, collaboration, maturity and procedural models, organisational success factor, hindering / success factors, modern cybersecurity threats, municipal cybersecurity, human factors, responsible for cybersecurity
Asia Pacific and	8	security in public sector organisations, national strategies,

research location	amount	research field
India		collaboration, metrics, success factors
Emirates	1	security in public sector organisations

In the following, we summarise the most cited literature that examines obstacles to the development of an ISMS:

Human factors are, therefore, a critical success factor. In their study, the authors *GLASPIE* and *KARWOWSKI* (Glaspie and Karwowski, 2018) focus precisely on these human factors in information security culture and found that the human factor is always the weakest link in enforcing measures and that this aspect must be optimised. After a systematic analysis, the authors concluded that the following human factors form the basis of a successful safety program: Information Security Policy, Deterrence, Incentives, Attitude, Commitment, Training and awareness, and management support. The authors also concluded that only technology-oriented security controls fall short. In addition, people at all levels of the organisation have an essential role to play in establishing a positive information security culture. They must be taken into account in any security program.

These findings also make *PREIS* and *SUSSKIND* (Preis and Susskind, 2022, p. 617) provide a good overview of the problems of the public sector and the costs that can accompany cyberattacks. In their work, the authors focus on the retro-perspective analysis of different studies regarding the cybersecurity status quo in American communities. The results are summarised here: Only a few local governments have developed or established such cybersecurity strategies in their administrations. Furthermore, cybersecurity risk management in the administration is weak or non-existent. Lack of financial and human resources is an obstacle to improving cybersecurity. Hardly any local government in the field of investigation has set up an ISMS with an external certification or operates a continuous improvement process.

To complicate matters, according to *NORRIS* (Norris et al., 2019, p. 896), the majority of American local governments suffer from permanent cyberattacks and, at the same time, operate their IT infrastructure with weak and poorly trained staff, and it is precisely of these administrations that the management level rates their cybersecurity management as "good to very good". This picture is confirmed in further studies in American local and city governments (Hatcher et al., 2020). In the United States and Europe, local government employees are poorly trained in cybersecurity, note the authors *ABANAS* and *NIKOLINA* (Arbanas and Žajdela Hrustek, 2019).

The human factor in the current cybersecurity landscape is also discussed by *BENSON* et al. investigate (Benson et al., 2019). Based on a systematic literature review, the authors outlined the most critical factors in constructing an ISMS in human factors, namely consciousness, individual attitude, norms and cultural context.

In contrast, *JALALI* et al. (Jalali et al., 2019) the organisational perspective of cybersecurity in the health sector. The study followed a systematic literature review and focused on the key aspects necessary for a successful healthcare strategy. The focus is on organisational factors, including the technical readiness of healthcare facilities. The factors identified in this study are software development security, Emergency plans and Planning and business continuity.

AWAN et al. (Awan, 2017) have examined the concrete measures of security strategies that influence the success of the implementation of such strategies. After a systematic literature review, the following factors were highlighted: The level of critical information infrastructures (CII), the level of protection already achieved, and the sharing of cybersecurity information.

The authors *KHANSA* et al. (Khansa et al., 2017) conducted a structured survey to examine the impact of organisational control in the cyber environment. The study explored the relationship between employee cyberloafing and formal organisational control. Cyberloafing is the use of internet access provided by the employer for private information gathering, private e-mail use or other online communication during working hours (Lim and Teo, 2005, p. 1081), (Vitak et al., 2011, p. 1751). Such behaviour negatively impacts productivity and can lead to unwanted and severe security issues. The study suggests that factors such as attitude, subjectively perceived norms, behavioural controls, and lack of punishment must be focused. These factors play an essential role in designing organisational controls, which must be considered when setting up and establishing an ISMS or CSS.

In addition to these factors, the chosen strategy and the procedural model also impact success. *COOKE* tries to identify the successful strategies for building a cybersecurity strategy in the public sector as part of his literature review (Cooke, 2017). In essence, the study provided the result that employees with good IT skills, adequate resources for the ISMS or CSS, corresponding internal guidelines and target group-specific educational programs are indispensable as a guarantee for a successful strategy.

This is followed by *NIKOLOVA'S* research work (Nikolova, 2017). Building on more than six years of experience in the Ministry of Information Technology and Communications, the author describes a method for target-group-specific training of employees and managers. The main finding of the multi-year project is that the widespread use of the presented method has significantly improved cybersecurity within the organisation. Target group-specific security measures, supported by suitable learning systems, are a success factor for increasing cyber resilience.

Similarly, research is being carried out in the Netherlands into the impact of different awareness-raising campaigns on employees (van Steen and Deeleman, 2021). The campaigns, which only distribute information to workers, do not have much impact on workers' behaviour. Therefore, the authors developed an educational game. An analysis

showed that employees better accept such learning games. Thus, a more significant contribution can be made to cybersecurity. At the same time, this analysis also underpins the fact that learning systems adapted to the employee are a success factors for resilience.

Researchers *CHOEJEY* et al. (Choejey et al., 2016) examined the critical success factors for cybersecurity in government organisations in Bhutan. The authors conducted a questionnaire-based survey. The study identified several critical factors that could be used to successfully implement information security. For the Cybersecurity strategy are essential, namely: Employee awareness of the ISMS and CSS as well as target group-specific training, preparation and publication of security policies, provision of the necessary budget, internal audits, definition of safety responsibility, establishment of an appropriate organisational structure, change management as well as communication and collaboration.

Also interesting is the work of *TATIARA* et al. (Tatiara et al., 2018). The authors determine the impediment factors in the implementation of an ISMS and thus delimit the necessary foundations from the organisation's point of view. For this purpose, expert interviews were conducted to confirm the data obtained from the literature. As a result, the following seven key factors were identified: 1. Involvement of top management through management reviews, 2. Informing employees about weak points or security incidents, 3. Review of the implementation of recommended security measures, 4. Communication of the improvement plan, 5. Communication of roles, including their tasks, rights and obligations, 6. Definition of work packages regarding the operating of an ISMS and 7. Create and publish guidelines and work instructions.

The authors *HUI-LIN* and *KUEI-MIN* also examine critical success factors in the introduction of an ISMS. In essence, four main groups were identified that significantly contribute to the successful development and sustainable establishment of an ISMS. These four main groups, "Guidelines and project management", "Project coordination", "Project monitoring", and "Management review", follow essentially the Deming circle (Plan-Do-Check-Act) and are founded by corresponding subgroups (so-called sub-critical factors). The results and key factors already described by the studies above are confirmed again (Hui-Lin and Kuei-Min, 2014).

Another aspect that should not be forgotten when setting up an ISMS is the procurement and provision of structured information regarding weak points of IT systems or software and their evaluation and provision for hazard prevention. *CHAINEY* and *BERBOTTO* (Chainey and Alonso Berbotto, 2022) illuminate in their article the possibilities of obtaining information with the help of so-called OSINT programs. OSINT stands for Open-Source Intelligence, i.e. obtaining information from freely available sources. *HWANG* et al. are researching in the same direction (Hwang et al., 2022). In addition to a well-founded introduction to OSINT, the authors describe the process for identifying, collecting and evaluating data from public sources. As a result, they shed light on the importance of OSINT from a cybersecurity

perspective and find that in a successfully implemented and operated OSINT environment, it is much more difficult for attackers to carry out cybercriminal activities. Another critical success factor, following *Potter* and *Hurley*, is the involvement of the Chief of Financial Office (CFO) in the procurement and distribution of information (Potter and Hurley, 2020). Hence, the CFO must be embraced and incorporated as a full-fledged participant in cyber efforts and an architect of the organisation's cybersecurity strategy. The CFO must have access to reports highlighting cybercrimes and attacks on varied information technology (IT) infrastructure. In addition, the CFO needs to know how information is targeted and used, the level of risk and impact to potential targets, technique(s) used to perform the cyberattack, have an understanding of cyber insurance and whether it is relevant and appropriate to the organisation's needs; and establish a risk management framework to identify, prioritise, and assess risks that threaten cybersecurity.

Gedris et al. are researching in the same direction (Gedris et al., 2021). The work focuses on cyberattacks on cities and other public infrastructures and how employees react or should react to them. The authors highlight various learning elements that can be important for defending against cyberattacks. These essentially include the skills and ingenuity of the employees, information brokering and communication, emotional intelligence, holistic approach including risk management, preparation to mitigate the effect of cyberattacks and last but not least, the cybersecurity awareness of the employees. The factors of awareness, communication, and a holistic approach, including established risk management, are especially mentioned as critical success factors for implementing successful cybersecurity.

This is followed by the analysis and model development of a so-called Cyber Security Operations Center (SOC) by the two authors, *Majid* and *Ariffin* (Majid and Ariffin, 2021). The article describes the foundations for successfully implementing a SOC. In principle, a SOC is not mentioned as a success factor in developing an ISMS. However, it can significantly contribute to security in later sustainable operations and should be included in further consideration.

The paper of *Alkhudhayr* et al. (Alkhudhayr et al., 2019) focuses on the factors that affect the security of networks and the Internet of Things (IoT). The work compares different attacks on networks and IoT and their impact on information and cyber security. As a result, the authors make recommendations to increase the security of the study areas in the context of the cybersecurity strategy, namely: In addition to guidelines such as orientation and training measures regarding cyber security for employees, as well as the implementation of technical security measures.

Farrand and *Carrapico* (Farrand and Carrapico, 2022) note in their article that a considerable percentage of public infrastructure is controlled by the private sector, which is accompanied by dependence on external private sector actors. This marks an entirely new approach to cybersecurity, where the private sector outside the EU can be perceived

as a threat and foreign powers from which digital sovereignty must be protected. In summary, outsourcing or the associated loss of control are obstacles to developing an ISMS.

Furthermore, *Cubuk* et al. (Çubuk et al., 2022) examine the drivers of digitisation in Turkey before the study focuses on securing the IT infrastructures of public institutions. Establishing secure information systems, ensuring the proper operation of installed systems, and protecting them from external damage are all referred to as critical aspects of information systems management. As a recommendation of the authors, in addition to the efforts to create correctly functioning systems, the environment in which the devices are located, the way IT professionals and users can use a system, the service management processes and the question of failure of the systems, e.g. in the event of a natural disaster, the cybersecurity strategy, its implementation and maintenance should also be considered. In summary, this recommendation can be understood as the basis of any cybersecurity strategy.

A study by *Chodakowska* et al. (Chodakowska et al., 2022, p. 180) in Polish local governments confirms the abovementioned results. The lack of financial resources is also mentioned as an obstacle to increasing cybersecurity. Instead, according to this study, qualified employees and better IT equipment, both current hardware and software, play a significant role. It is also necessary to raise awareness of potential risks among civil servants, develop clear standards and procedures and ensure strict law enforcement.

In 2020, the European Commission presented the new EU Cybersecurity Strategy, a central, integrated component of the European Council for the Digital Transition Programme, the Economic Recovery Plan and the European Security Strategy, intending to lead efforts towards secure digitisation. The article by *Schmitz-Bernd* and *Chiara* (Schmitz-Berndt and Chiara, 2022) compares the cybersecurity laws of Germany and Italy, which were developed for concrete implementation in the two countries due to the EU cybersecurity strategy. Harmonised cybersecurity rules at the EU level are the most efficient way to increase cyber resilience. However, individual steps taken by Member States contradict the basic idea of a more coherent environment across the EU. Therefore, the quest for greater cyber resilience should necessarily be coordinated by Member States to avoid fragmentation. Derived on the municipal sector, this means more cooperation in cybersecurity. Despite the growing awareness of the various actors about their vulnerability to cyber threats, suitable guidelines, training, and processes are still scarce (“Raising Awareness of Cybersecurity,” 2022). The same applies to the necessary awareness of topics at the management and employee level (Schaberreiter, 2022, p. 17). The study of *Alyami* et al. confirms this finding and describes the SETA program as a training process to reduce security incidents due to a lack of employee awareness (Alyami et al., 2022).

The NIS Directive is the first horizontal legislation undertaken at the EU level to protect network and information systems across the Union (Markopoulou et al., 2019).

Markopoulou et al. clarify that such a directive is essential for Europe to increase basic infrastructures and that an appropriate organisation, namely ENISA (Europe's Union Agency for Network and Information Security), is responsible for Europe-wide coordination. However, the implementation of this guideline also at the vertical level up to the local governments can only succeed with a process model that translates the abstract specifications and concrete measures.

Forrester et al. (Forrester et al., 2022, p. 161) examine the strategies within Italian local governments to increase the cybersecurity awareness of employees within administrations. These authors also describe obstacles to the implementation of cybersecurity strategies. As a result of the investigation, the lack of qualified personnel is mentioned, and the lack of financial resources is listed. As in Germany and France, the lack of funding for cybersecurity measures is being reduced due to the dominance of small to medium-sized authorities and the simultaneously increasing demand for social services in these municipalities. Such administrations are more likely to be victims of cyberattacks (Romanovská and Piter, 2022, p. 282).

Cyber security is, therefore, a cost factor that must be taken into account in the operation of IT (Fedele and Roner, 2022). In such a threatening ecosystem, investments in cybersecurity have become critical for firms to ensure the integrity, confidentiality and availability of data assets and the business's survival. This explains why such investments have permanently entered the decision variables that any organisation should consider. Providing appropriate funds is, therefore, a critical success factor for increasing resilience.

In particular, the tight budgets in public administration led to new approaches to allocating financial resources where needed. This is where the article by *Zheng* et al. comes in (Zheng et al., 2019). They propose an optimisation framework that prioritises investment in security mitigations to maximise vulnerability coverage.

Kitsios et al. (Kitsios et al., 2022) state that the integration of easy-to-use risk management is another essential critical success factor in the construction of an ISMS.

Sengupta (Sengupta, 2022)explains that empowering management and other stakeholders with the correct information in the proper format at the right time helps to design and implement an ISMS that meets the requirements of all stakeholders. Against this backdrop, *Sengupta* demands target-group-specific information and, at the same time, describes this as a critical success factor for the security level.

In contrast, the authors *De Abrew* and *Wickramarachchi* (De Abrew and Wickramarachchi, 2021) focus on the organisational factors that affect the effectiveness of ISMS and list other factors in addition to those already listed here, such as: Funding (from the government), Legal and social implementation pressures as well as the willingness of employees to participate in the security process actively.

Susukailo describes which skills (Susukailo et al., 2022, p. 263) experts should have in the context of information and cyber security. Furthermore, he then explains a simple procedure model for setting up an ISMS (Susukailo et al., 2022, p. 264). However, the article remains abstract and essentially focuses on the risk assessment to be carried out for security assets to be identified, but it calls for an internal audit to be carried out concerning the implementation of the technical measures and a revision of the existing documents.

In addition to the work that only formulates singular demands to establish an ISMS within the organisation, *Rehbohm* et al. the necessary architecture of a federal state and its impact on the construction of an ISMS and a cybersecurity strategy (Rehbohm et al., 2022b, p. 301). The authors describe a suitable architecture in a federal state as an essential component of the cybersecurity strategy. This is where the foundations for proactive cooperation on cybersecurity need to be laid, namely: Networking of participants, Exchange of information, Establishment of a single point of contact (SpoC), and Creation of the legal framework.

This argument is followed by *Taddeo's* study (Taddeo, 2019, p. 352). It defines cybersecurity as a public good that must be protected by appropriate architectures.

Poehlmann et al. (Poehlmann et al., 2021) list five key success factors regarding cybersecurity. First, the technical aspects, such as the usability of cybersecurity and the technological design process and its effects on cybersecurity, are examined. Second, the authors clarify that cybersecurity management is a never-ending process, from identifying, assessing, and responding to risks to managing continuous improvement. It is precisely this management process that must be integrated into an appropriate organisational structure in order to establish strategies to strengthen cybersecurity and, at the same time, reduce the costs of cyber-attacks. Fourthly, the effects of the legal environment are examined. These significantly contribute to awareness of the need for cybersecurity in public administrations. Finally, these authors also refer to human factors as an essential success factor. Furthermore, the authors argue that, in addition to a purely theoretical consideration of background and success factors, case studies should also be considered to test methods or models more in practice and draw insights from them.

The authors *Sabtu* and *Mohamad* compare the national process model of the Malaysian public sector with that of the National Institute of Standards and Technology (NIST) and other organisations and derive 21 success factors for the development and establishment of an ISMS (Sabtu and Mohamad, 2021, p. 375). In addition, the existing tools were analysed, and it was found that they only focus on or support singular problem areas such as training, risk management, threat scenarios, and information exchange platforms. In essence, this article provides recommendations that should be taken into account when developing a process model.

Nather's paper highlights several examples of how the U.S. government is using enterprise architecture (EAM) and risk management (RM) integration to identify, mitigate, and address risk scenarios (Nather, 2018). The author notes that EAM and risk management are often

considered and implemented in isolation. This hinders the development of ISMS, as it is much more challenging to integrate information security into the organisational strategy, business processes, information flows and technological decisions without EAM and risk management.

The development of a process model is one side of the medal. Another key point is measuring the resilience of infrastructures in the context of cybersecurity. Against this background, *CLEMITH* and *SICKER* investigated maturity and process capability models and their application to measure resilience in the public sector. The authors describe the absence of a maturity model as a hindrance factor in developing process models to increase the cybersecurity of public infrastructures (Clemith and Sicker, 2014).

The authors *KÄVRESTADT* et al. (Kävrestad et al., 2021) found in their study that the usability of cybersecurity is another success factor and, at the same time, forms the foundation for increasing the resilience of information security.

Usability is a success factor for the successful implementation of measures to increase information security. As part of a study carried out by *KOZA*, further hindering factors and success factors for the sustainable establishment of information security in rganisations were identified (Koza, 2021, p. 824ff).

The main obstacles identified were the high personnel resources, ambiguities in legal requirements (compliances), increased internal and external effort, complexity of IT systems, lack of frameworks for IT architecture and the digital carelessness of employees. On the other hand, there are the factors that help to establish an ISMS successfully: Sufficient personnel capacities, efficient tools (Hanschke, 2020b, p. 77ff) (ISMS-Tools), training and further education measures of the specialist staff, use of best practices, global knowledge management in the organisation, synergies through integrated management systems and last but not least state financial support.

It is striking that since the beginning of the 2020s, the number of publications in information and cyber security has risen sharply. In particular, there is great interest in the public sector.

4 Summary of Publications – Research Contributions

4.1 Selection of Research Contributions

This chapter lists the publications that are relevant to this dissertation (Table 8). These publications can be found in the subsequent chapters (marked in **green** here).

In addition, other contributions by the author are not part of the present dissertation. These posts have laid the foundations for the research work (marked in **grey** here) and are cited at the appropriate point.

Prof. Dr. Kurt Sandkuhl has contributed as a co-author to the leading publications. He subjected all contributions to a critical examination as part of this collaborative process. In particular, the research methodology used and the content were examined and reflected accordingly through feedback.

Since there were also overlaps in content with a field of research by another researcher from the same chair, some publications were produced jointly by Frank Moses and Thomas Rehbohm. Both authors' publications contain essential foundations in their research work or dissertations.

The posts were created and published between 2022 and 2024. The order in the list below is not identical to the order of publication of the individual publications.

Table 8: Publications

#	Title	Reference / Publishing body
1	Empirical Study on the State of Practice of Information Security Management in Local Government **(Section 5)**	**(Moses et al., 2022a)** Moses, F., Sandkuhl, K., Kemmerich, T., 2022a. Empirical Study on the State of Practice of Information Security Management in Local Government, in: Zimmermann, A., Howlett, R.J., Jain, L.C. (Eds.), Human Centred Intelligent Systems, Smart Innovation, Systems and Technologies. Springer Nature, Singapore, pp. 13–25. https://doi.org/10.1007/978-981-19-3455-1_2
2	CISIS12	**(Moses and Rehbohm, 2022a)** Moses, F., Rehbohm, T., 2022. CISIS12. kes, CISIS12.
3	Information security management in German local government **(Section 6)**	**(Moses et al., 2022b)** Moses, F., Sandkuhl, K., Kemmerich, T., 2022b. Information security management in German local government. Presented at the 17th Conference on Computer Science and Intelligence Systems, pp. 183–189. https://doi.org/10.15439/2022F162
4	Mit CISIS12 ein ISMS aufbauen **(Section 7)**	**(Moses and Sandkuhl, 2022)** Moses, F., Sandkuhl, K., 2022. Mit CISIS12 ein ISMS aufbauen. DuD Springer 46, 654–659. https://doi.org/10.1007/s11623-022-1677-5
5	Federal Cybersecurity Architecture and Information Security Management – Adoption and Diffusion of the NIS-2 Requirements **(Section 8)**	**(Moses and Rehbohm, 2023b)** Moses, F., Rehbohm, T., 2023a. Federal Cybersecurity Architecture and Information Security Management - Adoption and Diffusion of the NIS-2 Requirements, in: Auth, G., Pidun, T. (Eds.), GI Edition Proceedings Band 341 6. Fachtagung Rechts- Und Verwaltungsinformatik (RVI 2023). Gesellschaft für Informatik e.V., Bonn.
6	Föderale Cybersicherheitsarchitektur und Informationssicherheitsmanagement im Kontext der NIS-2-Richtlinie	**(Moses and Rehbohm, 2023a)** Moses, F., Rehbohm, T., 2023b. Föderale Cybersicherheitsarchitektur und Informationssicherheitsmanagement im Kontext der NIS-2-Richtlinie. Datenschutz Datensicherheit DuD 47, 648–655. https://doi.org/10.1007/s11623-023-1837-2
7	ISMS in Small Public Sector Organisations: Requirements and Design of a Procedural Approach	**(Moses and Sandkuhl, 2023)** Moses, F., Sandkuhl, K., 2023. ISMS in small public sector organisations: requirements and design of a procedural approach, in: Morichetta, A., Buchmann, R.A., Sandkuhl, K., Seigerroth, U., Kirikova, M., Møller, C., Forbrig,

#	Title	Reference / Publishing body
		P., Gutschmidt, A., Ghiran, A.-M., Marcelletti, A., Härer, F., Re, B., Johansson, B. (Eds.), Joint Proceedings of the BIR 2023 Workshops and Doctoral Consortium, CEUR Workshop Proceedings. Presented at the BIR 2023 Workshops and Doctoral Consortium, CEUR, Ascoli Piceno, Italy, pp. 1–10.
8	Entwicklung eines modularen ISMS und DSM	**(Moses and Rehbohm, 2023c)** Moses, F., Rehbohm, T., 2023c. Entwicklung eines modularen ISMS und DSMS. Datenschutz Datensicherheit DuD 47, 721–726. https://doi.org/10.1007/s11623-023-1850-5
9	CISIS12-Modell: In zwölf einfachen Schritten zum ISMS	**(Moses and Rehbohm, 2023d)** Moses, F., Rehbohm, T., 2023d. CISIS12 für kleine und mittelständische Organisationen IN ZWÖLF SCHRITTEN ZUM RECHTSKONFORMEN ISMS. IT-Sicherheit 14–19.
10	Information Security Management in Small Public Sector Organisations: Requirements and Design of a Procedural Approach **(Section 9)**	**(Moses and Sandkuhl, 2024a)** Moses, F., Sandkuhl, K., 2024. Information Security Management in Small Public Sector Organizations: Requirements and Design of a Procedural Approach. Complex Systems Informatics and Modeling Quarterly 54–68. https://doi.org/10.7250/csimq.2023-37.03
11	Information Security in small Public Sector Organisations: Design and Evaluation of a procedural Approach **(Section 10)**	(**Moses and Sandkuhl, 2024b)** Moses, F. and Sandkuhl, K. Information Security in small Public Sector Organisations: Design and Evaluation of procedural Approach, in Proceedings of Ninth International Congress on Information and Communication Technology, X.-S. Yan, R. S. Sherratt, N. Dey, and A. Joshi, Eds., London: Springer, 2024.
12	CISO as a Driver of an ISMS in Public Sector Administrations **(Section 11)**	**(Moses and Sandkuhl, 2024c)** Moses, F., Sandkuhl, K. CISO as a Driver of an ISMS in Public Sector Administrations, in *Human Centred Intelligent Systems. Proceedings of KES-HCIS 2024 Conference*, A. Zimmermann, R. Schmidt, L. C. Jain, and R. J. Howlett, Eds., Springer, 2024.
13	Risikomanagement in der öffentlichen Verwaltung	**(Moses, 2024)** Moses, F. Risikomanagement: Fundament einer GRC-Gesamt-Architektur, DuD Springer, pp. 442–449, Jul. 2024. https://doi: 10.1007/s11623-024-1954-6.

4.2 Research Methodological Classification

Within the framework of this dissertation, a mix of methods was used concerning research methods (Venkatesh et al., 2013). Both qualitative and quantitative research methods were used.

Since the thesis pursues a design goal, the focus is on qualitative research methods. Design-oriented research (Design Science Research) is an established and accepted research method in German business informatics that deals with constructing and evaluating artefacts (Hevner et al., 2004). With the help of these artefacts, questions from the research domain of business informatics are to be explained and solved (Wilde and Hess, 2006). The artefacts generated during the research work are usually information systems at their core. Typical research methods are case study research, modelling, prototyping, laboratory simulations, induction and deduction (Österle et al., 2010; Wilde and Hess, 2006).

Design-oriented research attempts to generate design approaches and innovations in the development and operation of information systems. This is done through reference, prototypes, guidelines, process, or even business models (Österle et al., 2010).

Of the publications listed in the table, the first article sheds light on the **status quo of information security in the research domain** (These publications can be found in the subsequent chapters (marked in **green** here).

In addition, other contributions by the author are not part of the present dissertation. These contributions have laid the foundations for the research work (marked in **grey** here) and are cited at the appropriate point.

Prof. Dr. Kurt Sandkuhl has contributed as a co-author to the leading publications. He subjected all contributions to a critical examination as part of this collaborative process. In particular, the research methodology used and the content were examined and reflected accordingly through feedback.

Since there were also overlaps in content with a field of research by another researcher from the same chair, some publications were produced jointly by Frank Moses and Thomas Rehbohm. Both authors' publications contain essential foundations in their research work or dissertations.

The posts were created and published between 2022 and 2024. The order in the list below is not identical to the order of publication of the individual publications (Table 8).

Contributions 2 to 11 explicitly deal with developing **a process model** and a related application system and can thus be assigned to design-oriented research.

Publications 12 and 13 shed lights on two topics that require special attention in the research field of "public administrations" within the present dissertation. First, **the CISO** plays a necessary role as an organisation's information security driver. Secondly, **risk**

management is only rudimentarily focused on considering those responsible due to the unique framework conditions in public administration. However, the research has shown that both topics have a corresponding relevance for successfully introducing an ISMS, so the collected findings have been documented in two separate publications.

The following table provides an overview of the research methods used in the research contributions of this dissertation, which are listed above (Table 9). The application of the individual methods is not explained in detail here, as this would go beyond the scope of the work. Furthermore, the methods are briefly described in the respective publications. In addition, references are made to the literature on research methods.

Table 9: Research-Methodology and Publications

	Publication #													
Research Methodology	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**further Literature**
Systematic Literature Analysis	X	X								X				(Dibbern et al., 2004; Fettke, 2006; Recker, 2021; vom Brocke et al., 2009; Webster and Watson, 2002)
Design Science (Prototyping)		X		X	X		X	X	X	X	X			(Goldenson and Gibson, 2003; Hevner et al., 2004; March and Smith, 1995)
Further qualitative Analysis (e.g. Cluster Analysis)			X	X							X	X	X	(Myers, 2019; Recker, 2021; Sidorova et al., 2008; Wilde and Hess, 2006), (Zerres, 2021), (Borchardt and Göthlich, 2009), (Diethelm et al., 2010)
Interviews	X		X								X	X	X	(Bortz and Döring, 2006; Walsham, 2006; Wilde and Hess, 2006)
Case Studies			X											(Robra-Bissantz and Strahringer, 2020), (Benbasat et al., 1987), (Walsham, 2006)
Labor & Field Experiments			X											(Kubbe, 2020)
Prototyping			X			X	X			X				(Goldenson and Gibson, 2003; March and Smith, 1995; Nugraha, 2020)
Reference Modeling		X		X		X	X	X	X					(Becker et al., 2002), (Fettke and Loos, 2002)
eXperience Methodology		X												(Schubert and Bhaskaran, 2007)
Ethnography	X	X							X					(Ploder and Hamann, 2021; Wilde and Hess, 2006)

4.3 Regulatory Framework of Research Objectives and Publications

The individual publications aim to contribute to answering the research objectives (Section 1.2). Against this backdrop, the individual publications are classified in the following framework (Figure 24). In addition, the research questions are assigned to the individual contributions.

The order in the regulatory framework is not identical to the order of publication of the individual publications.

Figure 24: Framework - Research Question vs Publications

In the following, the individual contributions, their aim, and their published results are briefly summarized.

For a better overview, the publications are first classified in *HEVNER'S* Design Science Research process (Figure 25). The publications highlighted in green are in the summary, and the ones highlighted in blue are referred to in an appropriate place in this work.

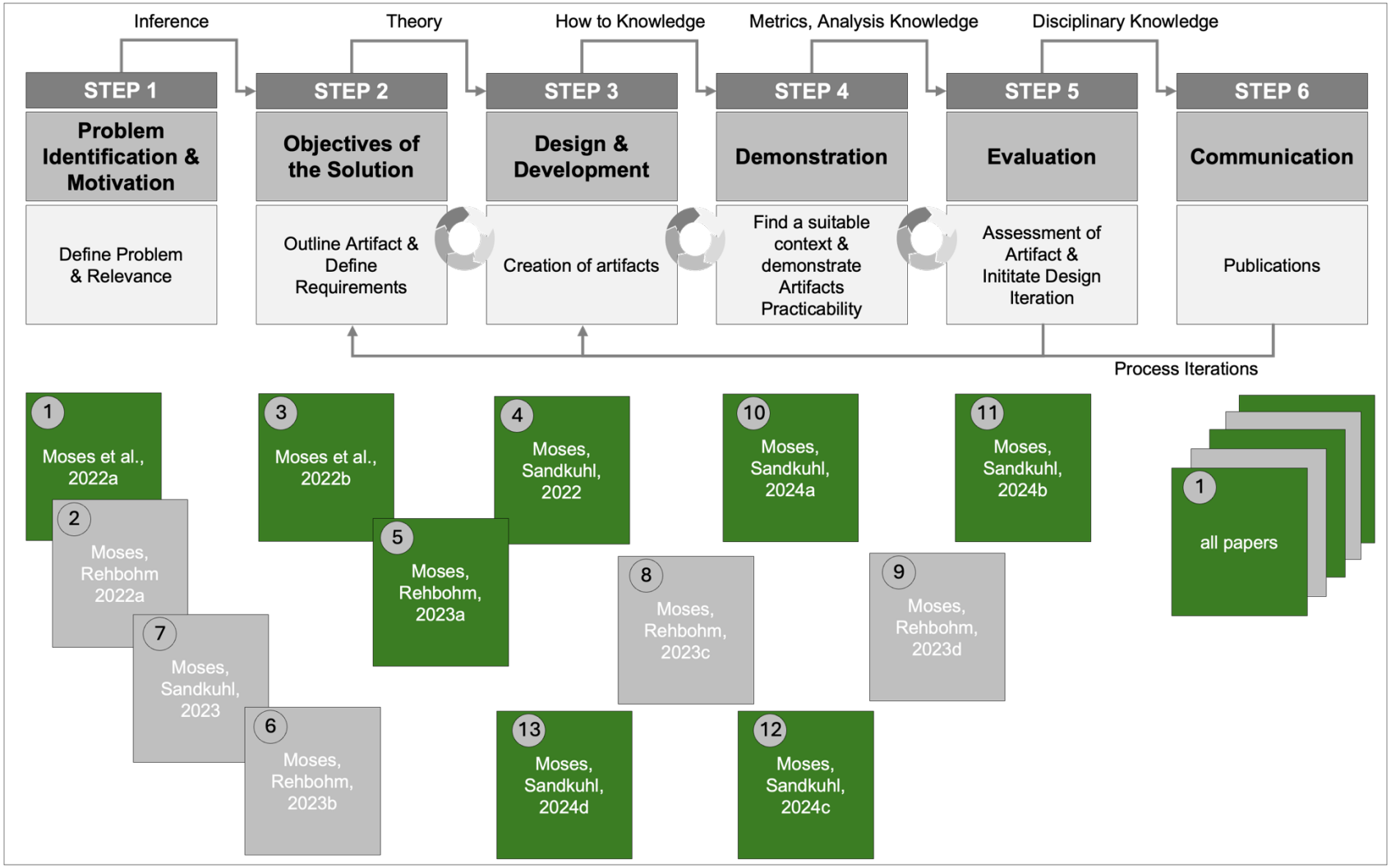

Figure 25: Overview DSR-Process and Publications

4.3.1 Publication #1 - Status Quo of Information Security Management in Public Administrations

This chapter summarizes Chapter 5 "Status Quo of Information Security Management in Public Administrations".

The research idea arose from the practical necessity for small to medium-sized local governments to develop a process model for implementing an ISMS. For this purpose, it was first and foremost necessary to learn more about the framework conditions and requirements of the research domain "local government".

With the help of an initial analysis, it was determined how many local governments exist in Germany and in which size classes they can be classified concerning the number of inhabitants. As of 31.12.2022, there were a total of **10,768** administrative units in Germany, which can be divided into the following size classes (Table 10): ("Destatis," 2024),(Heuermann et al., 2018b, p. 51)

Table 10: Municipalities classified by population

Municipalities with ... down to below ... Inhabitants	Amount	Cumulative Amount	% from 10.786	% cumulative
up to 100	202	202	1,87	1,87
100 – 200	449	651	4,16	6,03
200 – 500	1.423	2.074	13,19	19,22
500 – 1.000	1.705	3.779	15,80	**35,03**
1.000 – 2.000	1.838	5.617	17,04	**52,07**
2.000 – 3.000	1.005	6.622	9,31	61,39
3.000 – 5.000	1.175	7.797	10,89	72,28
5.000 – 10.000	1.372	9.169	12,72	85,00
10.000 – 20.000	906	10.075	8,93	93,40
20.000 – 50.000	516	10.591	4,78	98,19
50.000 – 100.000	113	10.704	10,4	99,23
100.000 – 200.000	42	10.746	0,38	99,62
200.000 – 500.000	25	10.771	0,23	99,86
500.000 and more	15	10.786	0,13	100,00

The focus of the research was on small to medium-sized local governments. It was found that around 35% of local governments are located in places where fewer than 1,000 inhabitants live. An extension of the scope of consideration to include municipalities with up to 2,000 inhabitants makes it clear that around 52% of municipalities in Germany can be divided into the class of "small to medium-sized" local governments. It is not uncommon for these micro-municipalities to only have a staff of a maximum of 20 employees (Schmid, 2019, p. 102).

However, all local governments must fulfil the contract matters (e.g., issuance of a federal identity card) (section 2.1). At the same time, all local governments, whether small or large, must comply with the same technical and safety measures. A prominent example is the Federal Motor Transport Authority (KBA) requirements regarding internet-based vehicle registration (i-KFZ), which require concrete measures for technical safety and the existence

of an ISMS. Failure to comply will result in exclusion from the group of users of the procedure (KBA, 2014).

After a rough definition of the research area "small to medium-sized" administrations, it was examined whether local governments have already demonstrably established an ISMS. For this purpose, certification companies for information security management systems certification were asked whether local governments had carried out corresponding audits and whether the associated audit reports could be evaluated.

The yield was sobering: Of the certification companies known in Germany, we only received a positive response from 2. The two certification companies provided 421 audit reports from 350 local governments from 2019, 2020 and 2021 for further analysis.

Table 11: Amount of analysed Audit Reports from Certification Bodies

Certification Body	Context	Number of audits
Federal Office for Information Security (BSI Germany)	BSI-Grundschutz	0
Cert Europe	ISO 27001	0
DQS	ISO 27001, ISIS	281
DEKRA	ISO 27001	0
TÜV	ISO 27001	0
IT Security Cluster	ISA+, ISIS	140

These 350 local governments were the **only** local governments from the two federal states of Bavaria and Saarland. In both federal states, funding programs have been launched by the respective state governments to increase cyber resilience, especially for local governments.

To evaluate the **421** audit reports, areas of investigation were coded in advance. With the help of these codings, an initial status quo of information security in the local governments examined could be ascertained.

Parallel to evaluating the audit reports, a study was conducted in the form of a structured interview with the 16 state commissioners of the federal states (CISOs) and a further 26 interview partners from state, city and local administrations. For this purpose, corresponding questions were used, directly related to the codings regarding the analysis of the audit reports.

The results obtained showed a high degree of unity. The results of the interviews conducted were better than those of the audits. This is probably because a self-perception is communicated during the interviews, whereas an external third party assesses the level of maturity during the audits. The figure below illustrates this picture and summarizes the rating of the codings with CMMI[2] maturity levels 1 and 2 in percentage terms (Figure 26). And it illustrates why 70 of the 350 local governments failed the audit on the first attempt.

[2] CMMI Maturity Level 1 = very bad, ..., 5 = very good

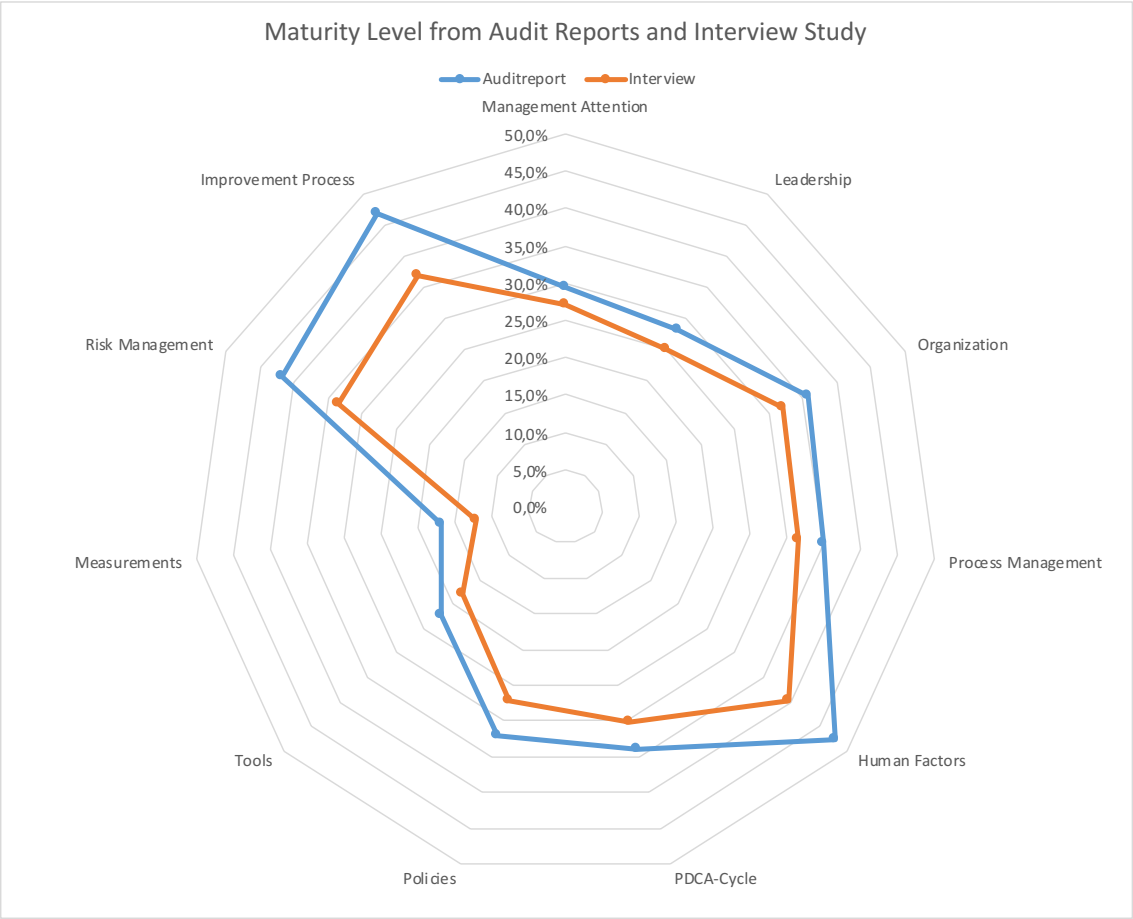

Figure 26: Maturity Level from Audit Reports and Interview Study

The deficits can thus be pinned down to the main areas shown in Figure 26. It is striking that around 30% of the interviewees have little management attention to information security. The same applies to the topic of leadership. Both points are probably also why the organizational structure and process management are only rudimentary in the local governments examined to establish an ISMS or operate it sustainably. The interviewees stated that there was sufficient staffing. Nevertheless, topics such as creating guidelines and service instructions fall short of expectations. The use of suitable tools was denied by most of the administrations examined, which is probably also responsible for the poorly rated implementation of appropriate measures. The willingness to establish a risk management system and an improvement process forms an essential foundation for further research work.

The following research results were achieved with the contribution:

- **Research Area**:
  - The spectrum ranges from 35% (3,779) to 52% (5,617) of German local governments.
- **Research Relevance**:
  - Considering the entire research area, only **3.25**% of the 350 local authorities out of 10,786 have demonstrably dealt with information security.

Conversely, this means that **96.75**% of German local authorities **have not yet** dealt with information security.

- **Research Result**:
  - Only a few local governments demonstrably deal with the topic of information security.
  - Many German local governments are poorly positioned in terms of cyber resilience.
- **Other Research Topics**:
  - What factors hinder or influence the implementation of an ISMS in local governments??
  - The planned process model for implementing an ISMS must address the deficient areas and optimize them sustainably!?
  - What are the unique features of the research domain?!?

In addition, the article "*Status Quo of Information Security Management in Public Administrations"* was able to answer the research question A1:

- "**A1. Determination of the Status Quo of Information Security in Small Municipal Administrations**".

4.3.2 Publication #2 - CISIS12 – Developing of a Prototype

This chapter summarizes Publication 2 "CISIS12".

The need to use a tool to set up and operate an ISMS was clear from the start of the research work and confirmed by the study and by analysing the audit reports.

Corresponding tools did exist on the market. However, these did not fulfil the requirements of the research domain. First and foremost, the software products established on the market were too expensive. Small local authorities can also not meet the high technical, organisational and personnel requirements (Markus and Meuche, 2022, p. 209).

Furthermore, the existing software products only support the introduction of ISMS based on IT baseline protection or ISO 27001. In addition, these application systems focus primarily on the framework conditions of private-sector companies, so these systems cannot be used in public administration and its framework conditions in general, nor in a small local authority in particular, without revision and customising.

Thus, a lack of appropriate tools can also be identified, in addition to the lack of a suitable process model for the research domain to introduce an ISMS.

With the analogy "chicken or egg, which came first?" the research work posed the question: "What is to be developed?"

- **Process Model and Application System**
  Development of a process model and parallel development of a prototype of an application system to support the process model while at the same time taking into account the requirements of the research domain.

  or

- **Process Model and Customizing of existing software products**
  Development of a process model and customising a software system established on the market and subsequent adaptation to the framework conditions of the research domain (if possible).

Since the requirements of the target domain can be better integrated into the development process, it seemed to make more sense to develop the planned process model, including supporting application software and subjecting both to an initial laboratory test as part of the research work. The results from the interview study and the analysis of the audit reports were integrated into this development process, and an initial approach to a process model and a prototype of an application system were developed using both an inductive and a deductive development process.

First and foremost, a framework containing all the key requirements for establishing an ISMS was created. As a result, a suitable catalogue of measures was developed through an iterative development process (Appendix A.1, A.2 and A.3).

In a further step, a suitable process model and supporting application software were created based on the framework's specifications.

The Bavarian IT Security Cluster, e.V., provides the framework and the catalogue of security measures.

This yielded the following results for further research work:

- **Research Area**:
  - The deficits identified by analysing the audit reports and the interview study were considered when developing the process model.
- **Research Relevance**:
  - Established process models such as BSI-Baseline Protection and ISO 27001 are unsuitable for small to medium-sized local authorities due to their complexity and high level of abstraction.
- **Research Results**:
  - Development and presentation of the artefact "Prototype of process model.
  - Development and presentation of the artefact "Prototype of the application system (M24S[3]“
  - Evaluation of the two artefacts as part of a laboratory test
- **Other Research Topics**:
  - Evaluation of the process model and the M24S application in a natural environment.
  - Further Development of the M24S application platform and adaptation to the requirements of the research domain.

Through the publication "CISIS12" and the associated research work, a contribution was made to answering the research question B3:

"**B3. Development of a software prototype to support the process model."**

With the help of this tool, the first laboratory tests have already been carried out to test the process model.

4.3.3 Publication #3 – Field Experiment with process model and software

With the help of project management methods such as Scrum® (Hron and Obwegeser, 2022; Schefferlie, 2020) the process model and supporting software could be quickly expanded.

[3] M24S is an abbreviation of the term **M**anagement Systems Solution**S**, where between the **M** and the **S** 24 letters are replaced by the number sequence **24**.

After the first laboratory tests with the software and the procedural approach, it was possible to supervise several real projects. As a result, 24 test administrations from four federal states (Bavaria, Saarland, Hanseatic City of Bremen and North Rhine Westphalia) were recruited to participate in the long-term study.

During the entire duration of the project, so-called "sprints" were carried out, taking into account the specifications of Scrum®. This made it possible to respond to change requests for the process model and the supporting software at short notice.

Thus, the following results were achieved by contribution #3 for further research work:

- **Research Area**:
  - The analysis criteria from contribution #1 could be integrated into the development process.
- **Research Relevance**:
  - As a result, it could be confirmed that the analysis criteria represent the foundation for further research and form essential requirements for the artefacts to be developed, namely the "procedural process model" and the "software".
- **Research Results**:
  - All 24 test clients could demonstrably improve in terms of the audit outcome on the one hand and thus also in terms of cyber resilience on the other.
  - In addition to local governments, the test group included a company and a utility company. At the same time, this ensured the universality of the research results and the artefacts presented (Benner-Wickner et al., 2020; Hevner et al., 2004).
  - The specific requirements of the research domain were made clear.
- **Other Research Topics**:
  - Further development of the M24S application platform and adaptation to the requirements of the research domain.
  - Optimization of the module catalogue of measures.
  - Creation of the possibility to use other module catalogues of measures in the application platform, such as BSI baseline protection.
  - Evaluating the growing data stock to generate decision support with the help of the data obtained.

Contribution #3 and the related research work contribute to a better understanding of the requirements of the research domain and answer part of the research questions A2, A3 and B2.

- „**A2. Determination of the characteristic features of local government. “**
- **„A3. Determination of the unique requirements, framework conditions and architectures for developing and establishing an ISMS in municipal administration. “**
- **„B2. Determination of relevant activities of the process model.**

4.3.4 Publication #4 – Initial Evaluation of the process model and the software

To fulfil Hevner's guideline "Design evaluation", the results from the previous articles were evaluated in detail in publication #4 and integrated into the further development of the process model.

The TOE framework by *TORNATZKY* and *FLEISCHER* forms the theoretical foundation for the development and continuous improvement of the process model (Tornatzky et al., 1990). As organisations are influenced by three specific mechanisms, according to *DIMAGGIO/POWELL*, the TOE framework with its levels of organisation, environment and technology was supplemented by the motivational levels of mimetic, normative and coercive pressure (DiMaggio and Powell, 1983).

The first result of the research work for article #4 is that external factors primarily motivate organisations to set up an ISMS. Secondly, there is mimetic pressure. On the other hand, coercive pressure arises due to external regulatory requirements such as the NIS 2 Directive. Finally, normative pressure occurs from established behaviour within a group or from a conviction.

As part of the pilot projects launched in 2020, the 24 pilot participants were asked about their motivation for introducing the ISMS. Figure 27 below provides an overview of the results of the interviews, which were also conducted in subsequent years with an increasing number of interviewees.

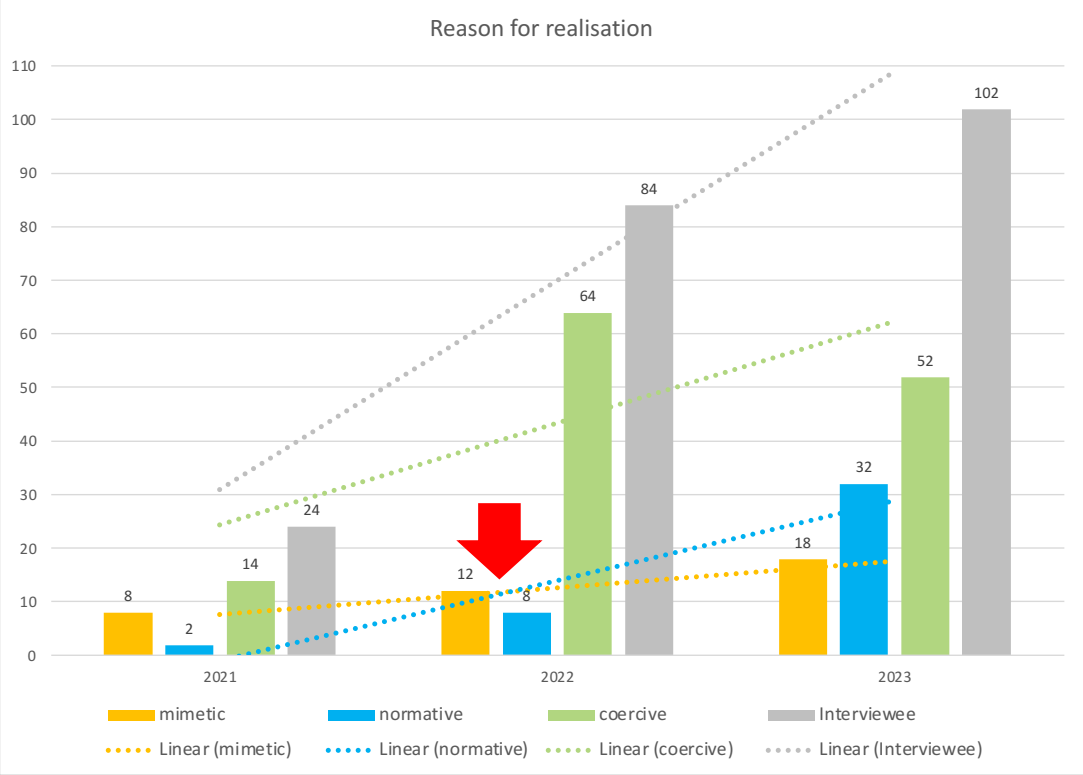

Figure 27: Reason for the realisation of the ISMS

Results Interview 2021:

- 8 organisations wanted to introduce the ISMS for mimetic resons (=33,3%, n=24).
- 14 organisations (=58,3%, n=24) stated they wanted to establish the ISMS due to existing support programmes (coercive reason).
- Only 2 organisations (=8,33%, n=24) can be identified as early adopters, i.e. opting for an ISMS on normative considerations.

After the pilot phase, the research project was extended to other clients. In 2022, a total of 84 organisations were already working with the process model and the application software to introduce an ISMS.

Results Interview 2022:

- 12 organisations stated that they decided to introduce an ISMS based on recommendations from other organisations (mimetic reasons) (=14,3%, n=84).
- 64 organisations (=76,2%, n=84) also decided to introduce an ISMS in 2022 only if they received appropriate support from a funding programme. This is a sharp increase compared to the previous year, which can be explained by the newly launched funding programmes in two federal states.
- Eight interviewed organisations (=9,5%, n=84) stated that they had introduced an ISMS for reasons of conviction or because security measures were essential for the organization.

In 2023, the number of users was further increased to 102 organisations. As part of further evaluations, the organisations were also interviewed in September 2023 regarding their motives for introducing an ISMS.

Results Interview 2023:

- 18 der organisations (17,6%, n=102) said they introduced the ISMS for mimetic reasons.
- Only around half (=50.9%, n=102) of the interviewees cited "support form funding" as motivation for introducing an ISMS.
- In contrast, the number of organisations that introduced their ISMS out of conviction rose to 32 organisations (=31,3%, n=102).

The increase in the number of organisations that introduce their ISMS for reasons of conviction on the one hand and the decrease in the number of organisations that only introduce their ISMS due to funding support on the other can be seen as a positive trend (red arrow in Figure 27). First and foremost, the interviewees cited the simple and intuitive process model, which enables a quick and accessible introduction to ISMS. At the same time, the geopolitical situation is contributing to a rethink at the management level, which has increased awareness of the need to establish an ISMS.

This is confirmed by the recently conducted study with 20 new software users. Only 3 organisations (=15%, n=20) stated that they were introducing the ISMS for mimetic reasons. As many as 15 of the new users (=75%, n=20) are introducing an ISMS out of a conviction that an ISMS is a must-have and the only way to ensure cyber resilience in the long term. Only 2 organisations (=10%, n=20) are introducing the ISMS because of the funding provided.

Based on TOGAF (The Open Group Architecture Framework), a general approach for designing, planning, implementing and maintaining organisational architectures, a process model was developed in an iterative development process. The phase and process structure of the process model reflects the four phases of TOGAF. TOGAF provides corresponding basic features but falls short in certain areas, particularly when adapting to the requirements of local authorities or small organisations.

At its core, the process model focuses on an organisation's assets. By working through the twelve steps presented, the ISMS is built up successively, thereby increasing the security of the assets and, at the same time, increasing the organisation's resilience.

With the help of the research carried out in Publication 4, the following results were achieved:

- **Research Area**:
  - Evaluation of the process model and the software in a natural environment.
- **Research Relevance**:
  - Alignment of the development to TOGAF.
  - Provide proof of the system's openness to the process model and the supporting software.
- **Research Results**:
  - First evaluation of the process model in a natural environment.
  - Determination of the motive structure for the implementation of the ISMS.
- **Other Research Topics**:
  - Further development of the M24S application platform and adaptation to the requirements of the research domain.
  - Ausbau, Ergänzung und weitere Optimierung der Template-Kataloge als Flankierung der Nutzer zum einfachen und schnellen Aufbau eines ISMS.

Publication #4 examines the process model's results in natural environments. It also sheds light on the opening for further catalogues of measures required in the process model and the software, thereby answering research question B.2.

- **„B.2. Determination of relevant activities of the process model.**

4.3.5 Publication #5, 6, 7 and 8 – Optimisation of the template catalogues

Contributions **#5-#8** address the interface between defining and implementing the requirements. Information security is part of cyber security (Section 2.2). The recently published NIS-2 Directive sets out new and additional requirements. The Network and Information Systems Directive 2 (NIS-2) is a European directive that aims to improve cyber security in critical infrastructure and digital services. It significantly expands the scope and obligations of the previous directive and provides various measures to achieve the goal of improved resilience (Weissmann, 2023). At the same time, fourteen requirements are formulated in Art. 21 of the NIS 2 Directive. These were analysed as part of the research work, and the effects were integrated into the further development of the process model. As a result, the existing process model was expanded in **publication #5** to include a cybersecurity architecture. This means that higher-level governance is now possible. At the same time, integrating a cyber security architecture requires appropriate interfaces between the information security management system and the cyber security architecture. Furthermore, the ISMS must offer the option of using catalogues of measures from different subject areas.

This is where further research work comes in. On the one hand, existing approaches are too complex (Markus and Meuche, 2022, p. 209) or only focus on a specific application context, e.g. BSI baseline protection or ISO 27001. The ISMSs set-up are inflexible, age quickly, and are often challenging to operate sustainably. The following requirements can be derived from this for further research:

- Development of an open process model,
- Mapping of the open procedure in the supporting software,
- Target group-specific asset and security measure catalogue,
- with simultaneous adaptation of these catalogues.

Die requirements aim

- to achieve better flexibility in both the process model and the software
- and thus lay a logical and physical foundation to ensure and facilitate adaption to future requirements.

This system openness makes it easier to set up the ISMS, ensures the sustainability of the established ISMS and, at the same time, guarantees system flexibility.

To do this, it was necessary to monitor and analyse the requirements from the research domain and generate new content with the data obtained. For this purpose, a data warehouse was connected to the database to support decision-making and the data was graphically processed with the help of a BI solution (Figure 28).

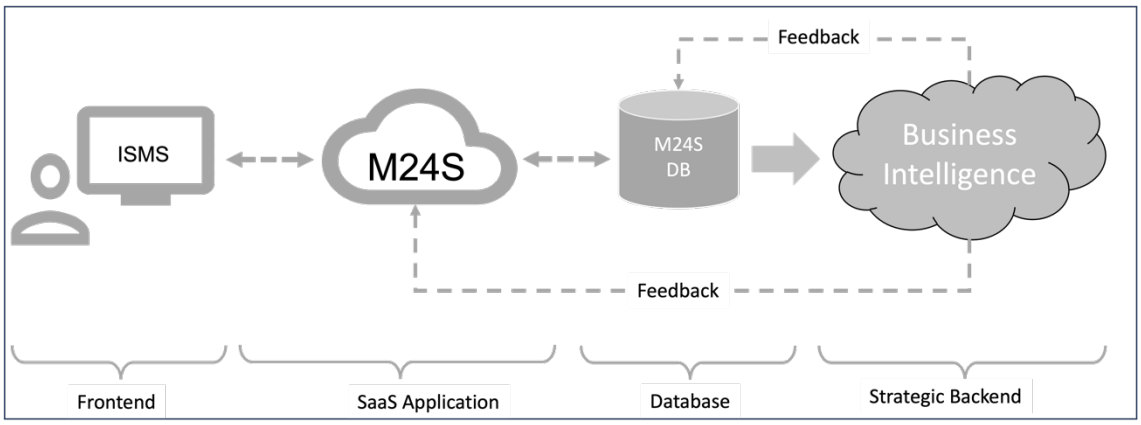

Figure 28: Process model with BI coupling

With the help of the transformation process (ETL) established in business intelligence (BI) systems, the constantly growing data stocks could be prepared by the ETL sub-processes of filtering, harmonisation, aggregation and enrichment in such a way that they could be used as a basis for decision-making (Kemper and Finger, 2016, p. 129ff), (Bauer and Günzel, 2013, p. 43)

Filtering is the **first** layer of the transformation. The data required for the data warehouse is selected in the M24S database at regular intervals with the help of a scheduler in a two-stage process (extraction), temporarily stored in the data warehouse and freed from deficiencies there (cleansing).

Harmonisation forms the **second** layer of the transformation and provides initial data for the decision support process, although this is still at the most detailed level (granularity: very high). Due to the structured nature of the data in M24S, data from different M24S clients or client groups can be integrated into the data warehouse without the need for **syntactic** or **functional** harmonisation of the selected data in preparation for physical integration. The functional harmonisation optimises the desired granularity with the help of specific transformation rules to combine asset or security measure-specific values using aggregation mechanisms.

Once the transformation is complete, the data warehouse contains a cleansed and consistent database with suitable granularity that can be used directly to generate information (Kemper and Finger, 2016, p. 139).

The **third** transformation layer is used for **aggregation**. The filtered and harmonised data is combined into "cubes ", each cube dimension representing a specific criterion. These cubes can be used to generate various analyses and then to support decision-making (Totok, 2016, p. 36ff)

The figure below illustrates this transformation process (Figure 29).

The BI solution can seamlessly integrate into the overall process model and the associated application platform. Using the ETL process described above, the different content data is integrated into the data warehouse (filtering), then harmonised and aggregated accordingly

so that corresponding evaluations can be provided as decision support, for example, in a dashboard.

The evaluation is carried out by strategic business users and is fed back into the asset and safety measure catalogues and other templates available in M24S via feedback processes.

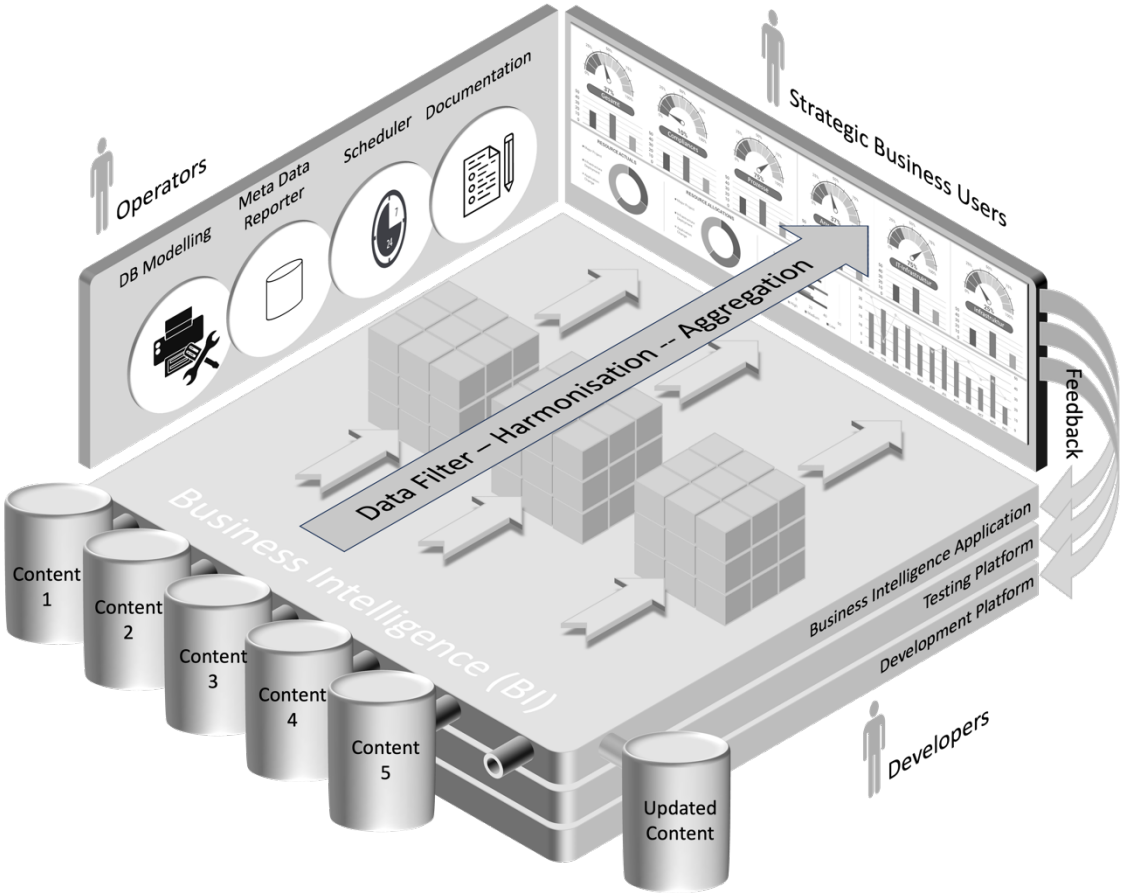

Figure 29: Business Intelligence Approach and Connection with M24S

The core task of decision support is the identification of

- new Assets without suitable security measures,
- customised security measures created by the single clients
- an asset with assigned individual security measures,
- overview of security measures for linked assets,
- degree of implementation of the individual security measures,
- outdated or no longer user security measures,
- generating of data as enrichment of the higher-level cyber security architecture,
- generating of data as feedback for the clients,

to recognise the constantly changing requirements on the one hand and to react to these changes with measures to be developed on the other.

First and foremost, feedback for the catalogue of safety measures was achieved with the help of the decision support system. Changes or new developments could be made available to the test clients quickly and easily via the SaaS application M24S.

By integrating external sources into the BI system, it was possible to respond to external requirements, e.g. the requirements of the NIS 2 directive, at an early stage.

Newly developed or modified target group-specific asset and template catalogues and new or adapted security measures were quickly and easily made available to the test clients via the SaaS application. This means that inexperienced users can also use the process model.

Thus, the following results were achieved by contributions #5, 6, 7 and 8 for further research work:

- **Research Area**:
  - Identify deficits in the security measures catalogue and new external requirements that affect the process model and the asset, template and security measures catalogues.
- **Research Relevance**:
  - On the one hand, environmental and technological dynamics require a process model that adapts to both external and internal requirements. On the other hand, external requirements must be identified and integrated into the process model and its catalogues.
  - Establishment of a data-driven approach as a foundation for further research work.
- **Research Results**:
  - A data warehouse and business intelligence include the appropriate tools for decision support.
- **Other Research Topics**:
  - Further development of the M24S application platform and adaptation to the requirements of the research domain.
  - Expansion of the data-driven approach with the help of BI tools for decision support.
  - Evaluation of the process model.

Publications 5, 6, 7 and 8 and the related research work contribute to a better understanding of the requirements of the research domain and answer a part of the research questions A2, A3 and B3.

- **„A2. Determination of the characteristic features of local government. “**
- **„A3. Determination of the unique requirements, framework conditions and architectures for developing and establishing an ISMS in municipal administration. “**
- **„B3. Development of a software prototype to support the process model. “**

4.3.6 Publications #9 and #10 – Requirements and Design of a Procedural Approach

Posts **#9** and **#10** pick up on the findings of the previous articles. The articles aimed to publish further research results and the further development of the process model and the supporting software.

As part of the further research, the focus was placed on determining the requirements for the successful implementation of an ISMS. On the one hand, the requirements of the NIS 2 Directive provide a legal framework that a process model and the associated information system must fulfil. In addition, there are further organisational, technical, financial and personnel success factors. These obstacles and success factors were identified with the help of a corresponding literature analysis and published in post #10.

As a result, 60 requirements were compiled from the literature that should be considered when implementing an ISMS. Specific requirements were already taken into account in the process model. Others could only be integrated into further research and development due to these new findings. This confirmed the alternating deductive and inductive research approach (Reinders and Ditton, 2011, p. 47).

However, it is essential that all twelve steps of the process model can be substantiated with the help of contribution #10 through the literature research carried out.

The core of **publication #9** contains the final description of the developed process model. Driven by the PDCA cycle, the five key topics of the process model are presented, under which the 12 steps of the process model are summarised (Figure 30).

The Bavarian IT Security Cluster, e.V, provides the framework and the catalogue of security measures and many helpful documents.

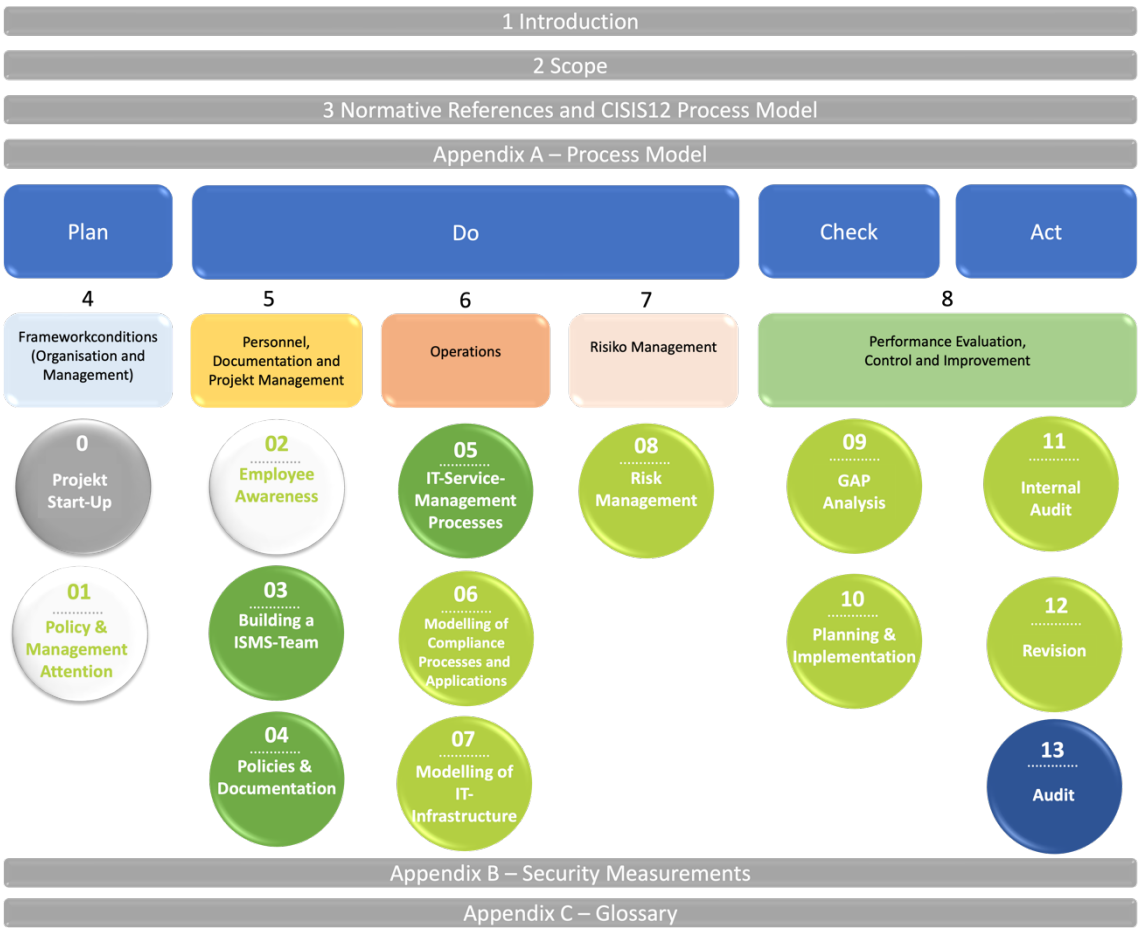

Figure 30: CISIS12-Approach - Classification in the PDCA cycle

When writing this dissertation, 251 organisations were using the procedure. The initially planned focus on small local authorities is still the focus of this research. The process model is now also being used by small and medium-sized enterprises, which hope to gain an accessible introduction to information security and thus increase the cyber resilience of their organisation, business processes and IT infrastructures.

The two charts below provide an overview of the scope and extent of the process model (Table 12, Figure 31). Figure 31 illustrates the influence of existing funding programmes (Bavaria and Saarland) on the willingness of organisations to introduce an ISMS.

Table 12: Users of the process model by industry

Sector	Amount
Health	5
Transport and Traffic	1
Finance and Insurance	1
Consulting	10
Information Technology and Telecommunications	2
Chemistry and Pharmaceuticals	1
Other commercial companies	15
Municipal Administrations	215
Research and Teaching	1
Sum	**251**

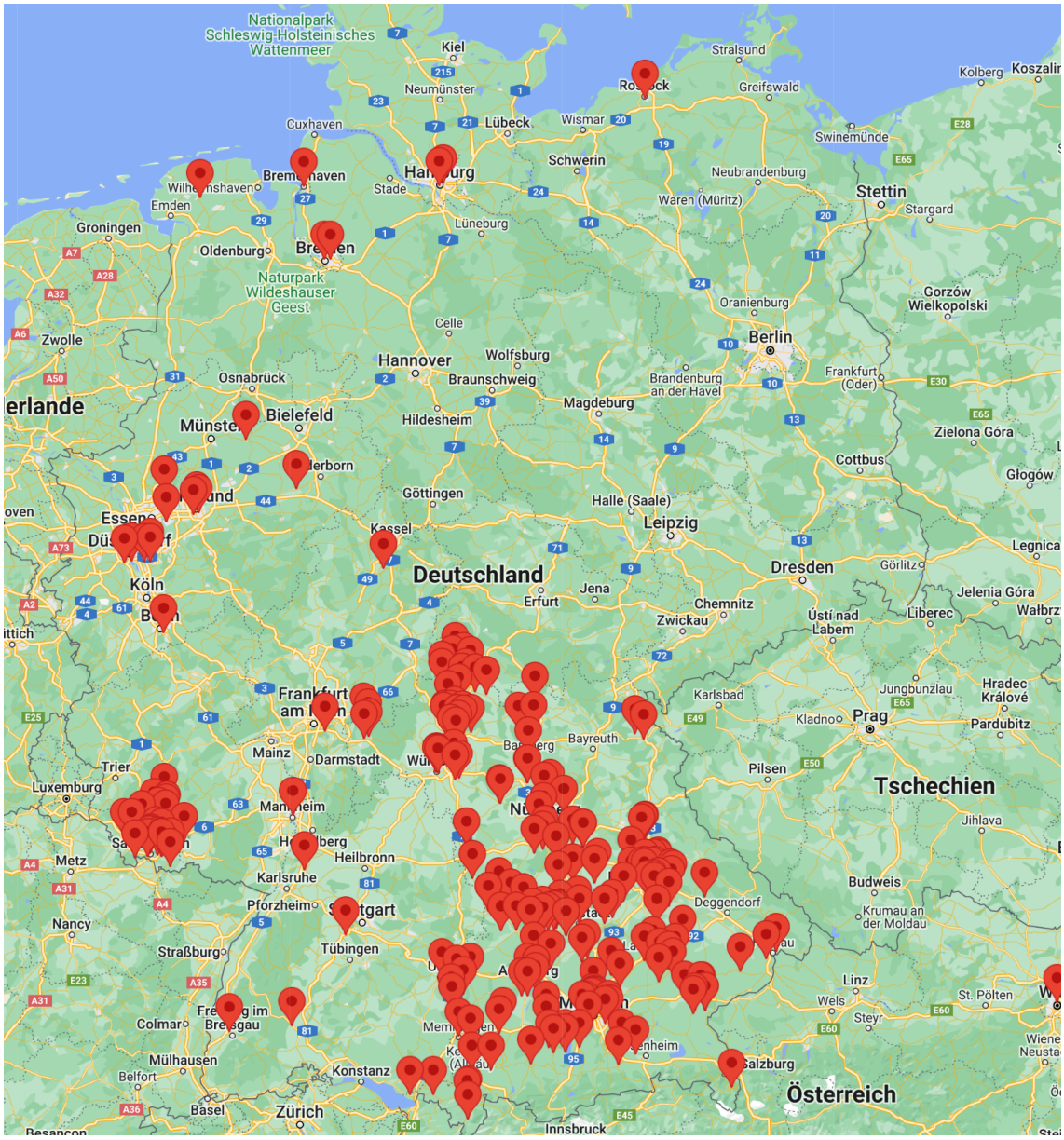

Figure 31: Spread or places of use of the process model

Thus, the following results were achieved by contributions #9 and #10 for further research work:

- **Research Area**:
  - The final description of the process model.
  - Proof that the process model can also be used outside the research domain.
- **Research Relevance**:
  - The number of organisations actively working with the process model illustrates its relevance to research.
  - The application outside the research area proves the general validity.
- **Research Results**:
  - The final description of the process model.
- **Other Research Topics**:
  - Development of template security measurement catalogues for SMEs.
  - Development of further template catalogues for local authorities in response to environmental and technological dynamics.

With the help of Publication #9 and #10, the research questions A3 and B2 could be answered:

- **„A3. Determination of the special requirements, framework conditions and architectures for developing and establishing an ISMS in municipal administration. “**
- **„B2. Determination of relevant activities of the process model.**

4.3.7 Publication #11 – Design and Evaluation of the Procedural Approach

Further research focuses on developing an evaluation strategy for the artefacts that have been developed. This evaluation strategy was developed based on the Framework for Evaluation in Design Science Research (FEDS) presented by *VENEABLE* (Venable et al., 2016) and published with **article #11** in the journal ICICT in early 2024.

Various evaluation episodes were carried out based on the evaluation strategy developed. Firstly, a literature review was conducted to identify the research gap and the problem. In a further step, a laboratory experiment was carried out to test the functionality of the process model and the software developed. The applicability was tested in a natural environment as part of further research. The clients mentioned in **article #3** were surveyed again regarding their experiences with the process model and the software (survey period March to May 2023).

Essentially, the **applicability**, **usefulness**, **comprehensibility** and **accessibility** of the artefacts were demonstrated through the various evaluations. These results were integrated back into the further development process, both for the process model and the software.

Although the chosen evaluation strategy was helpful, the evaluation process was nevertheless associated with some difficulties. On the one hand, there was a lack of methodological guidance on which target criteria and combinations of methods are helpful for an evaluation or when a sufficient level of evaluation activities (saturation) has been reached. A self-selected mix of evaluation activities or episodes could solve these deficits.

To evaluate the developed process model, small public sector organizations using the procedural model were interviewed following a structured interview from October to December 2023. **162** organizations use the procedural model, all participating in the study. First and foremost, these are users from the local government. These are divided into small, medium and large organisations. As a result, we interviewed 333 people, directly or indirectly.

The interview aimed to have at least one interview partner from the C-level (management level), one person from the IT department and last but not least, the ISMS manager (CISO) from each client. As a result, **333** people were interviewed (Figure 32).

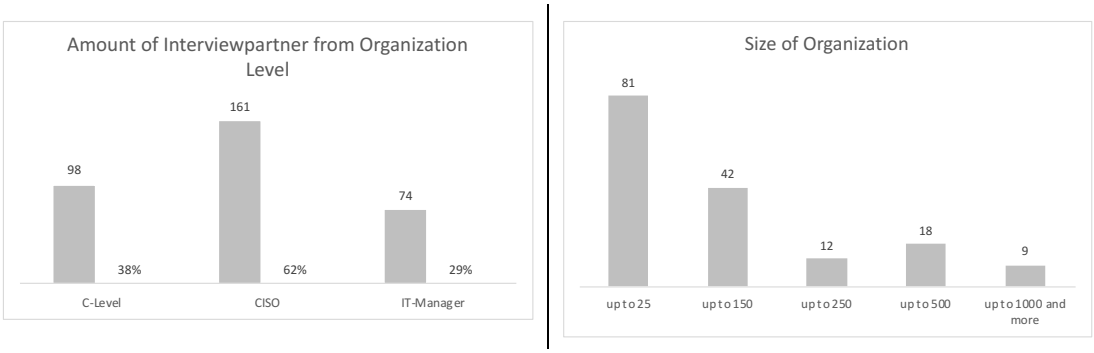

Figure 32: Size of Organisation and interviewees and amount from the organisation level

Since the research project has been running for some time, empirical data from a larger group of users with several years of experience are now available. The experience potential of the users thus ranges from a few months (clients from 2023 or early 2024) to several years of experience (first test clients from 2019).

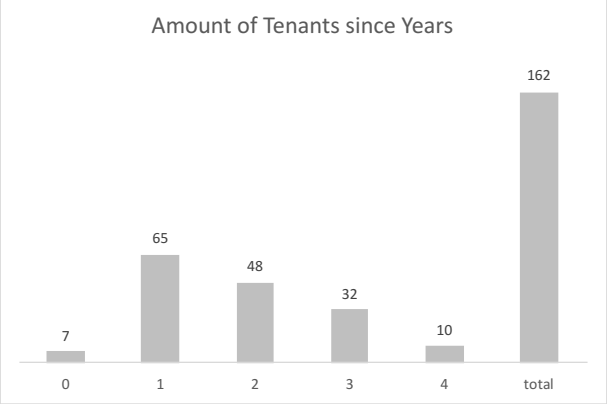

Figure 33: Amount of Tenants since Years (Experience)

A questionnaire with 20 questions was designed for the interview. The answer was made with the help of the CMMI-Maturity. The summary of the individual questions or answers of the individual interviewees is summarized in the following Table 13.

Table 13. Evaluation of Question with CMMI-Maturity in %

Question	1	2	3	4	5
Simplifying the implementation of an ISMS	0	0	0	61	39
Elimination of the mentioned hindering factors	0	0	2	50	48
Focus on the management's attention through step-by-step procedure	0	0	1	64	35
Focus on awareness of the employees (training measures)	0	0	4	38	58
Facilitate team-building activities	0	0	0	32	68
Simplification of the documentation task through precise specifications – Guidance	0	0	2	37	61
Simplification of modelling using templates and multiple measure catalogues	0	0	3	70	27
Easy integration of risk management on the modelled assets	0	0	11	59	30
CIP optimization takes place through internal and external audits	0	1	34	21	44
Increasing awareness of ISMS implementation in the organization	0	0	35	42	23
Simplification of concrete measure implementation	0	0	8	56	36
Simplified management integration into the ISMS process	0	0	7	74	19
Simple and intuitive tool	0	0	0	16	84
Structured and comprehensible procedure model	0	0	4	39	57
Ensure the sustainability of the ISMS	0	0	19	16	65
Better active control of the ISMS	0	0	15	52	33

Question	1	2	3	4	5
Implementation speed with the help of the procedure model	0	0	7	34	59
Increase the maturity of the ISMS as a KPI	0	0	18	26	56
The foundation of a cyber security architecture or Part of a cyber security architecture	0	0	7	63	30
Other positive side effects	0	0	20	21	59

In the following, the results of the individual questions are further examined. For this purpose, the individual interviewees' experience is considered for each question result. 9 exemplary questions are illuminated in this paper.

Simplifying the implementation of an ISMS

The question "Simplifying the implementation of an ISMS" is predominantly answered with "yes" or with a CMMI value of 4 (61% n=162) and 5 (39% n=162). If only the answers of clients operating their ISMS with the process model for 3 and 4 years are considered here, the trend becomes even more visible than for clients who have just started setting up their ISMS (Figure 34, Figure 35). This is primarily because some of these clients have not yet completed all steps of the process model in their entirety and thus cannot yet conclusively recognize or evaluate the positive effects of the process model. However, it can be stated that all interviewees confirm the simplicity of the process model.

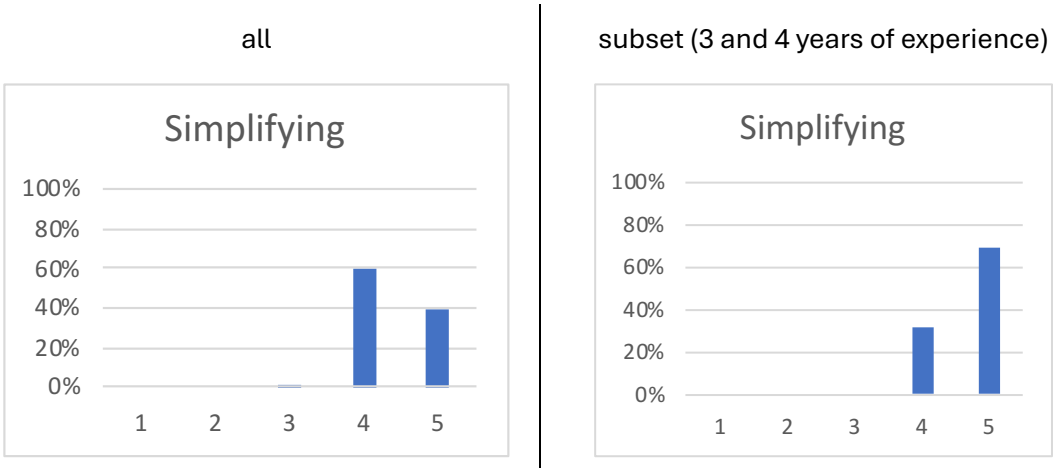

Figure 34: Simplifying the implementation of an ISMS (Clients with 3-4 years of experience)

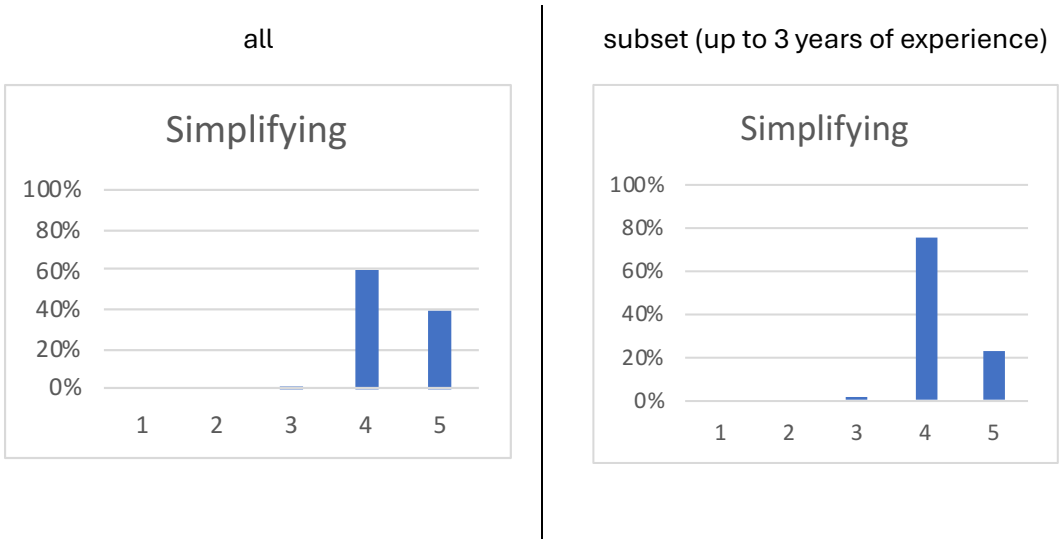

Figure 35: Simplifying the implementation of an ISMS (Clients with up to 3 years of experience)

Elimination of hindering factors

The impediments identified by the literature analysis were presented to the interviewees. Most respondents answered with a high degree of maturity when asked whether the process model helps eliminate or reduce these hindering factors (Figure 36). A further analysis of the respondents' experience confirmed the high degree of maturity: 3% of respondents rated the question with 3, 42% rated the question with 4 and 55% with 5 (n=115). The group that has only been using the process model for a short time or a maximum of 3 years also confirms maturity level 3 with 2%, maturity level 4 with 50% and maturity level 5 with 47% (n=115).

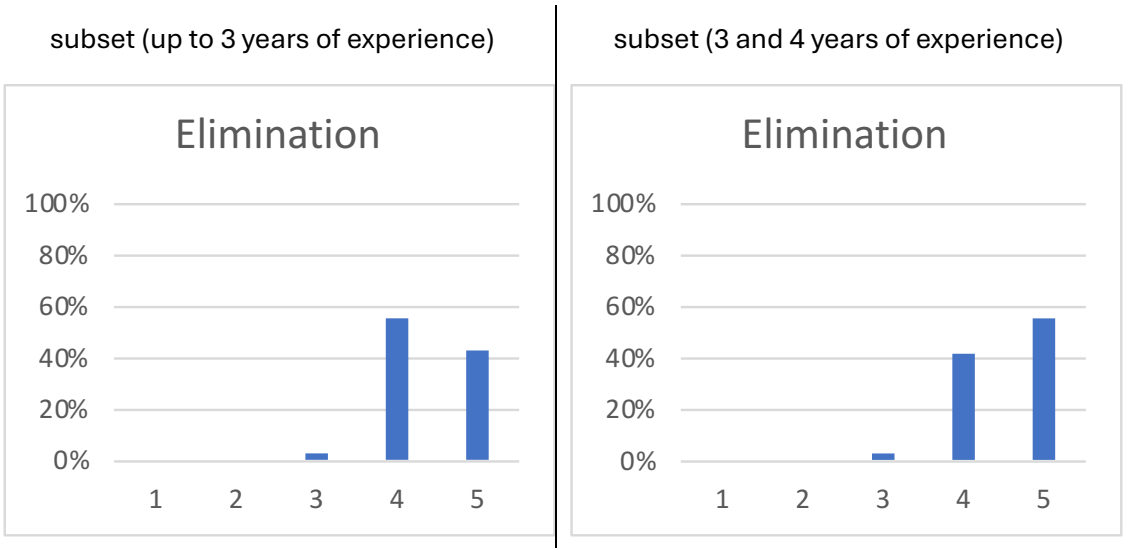

Figure 36: Elimination of the hindering factors (Clients from different experience groups)

Focus on the management's attention through step-by-step procedure

A similar picture emerges for "Management Attention" (Figure 37). The fact that the process model actively integrates the management level into the ISMS in step 1 ensures that management attention is available from the beginning of the ISMS project. At the same time, one of the hindering factors is eliminated. Both groups (up to 3 years and 4 to 5 years of experience) rate this question with a score of 4-5 on the CMMI maturity scale.

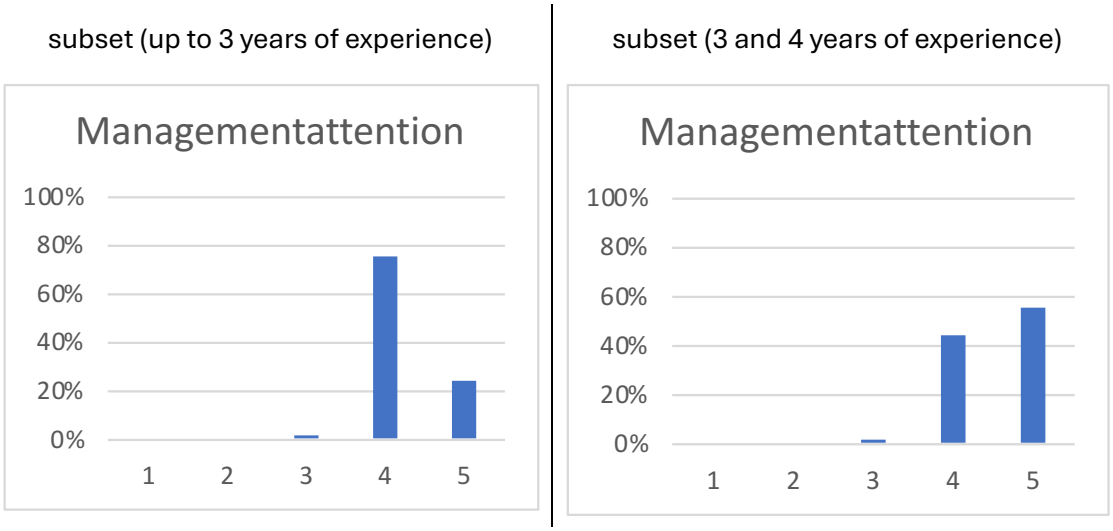

Figure 37: Focus on the management's attention

Focus on awareness of the employees (training measures)

One of the critical factors in introducing an ISMS is the training and awareness-raising measures of the employees. All respondents rated This question with great importance: 58% rate the training and awareness-raising measures with a grade of 5, 38% with a grade of 4 and only 3% with a grade of 3 (n=333). A look at the respondents' experience clarifies that clients who have already been working with the process model for 3 to 4 years see great importance in the training and awareness-raising measures (Figure 38). This is particularly true against the background of the investments in the ISMS, the desired resilience, and the continuous improvement process. For the group of respondents with a minimum of 3 years of experience, the importance of the training measures is also rated very high, but not yet at the same level as the comparison group (Figure 38).

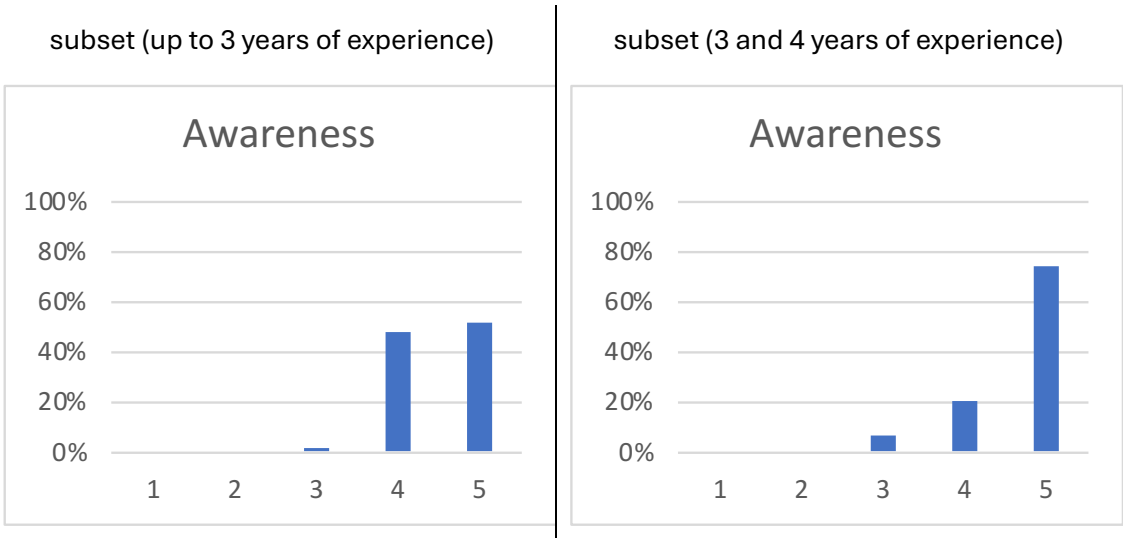

Figure 38: Focus on awareness of the employees

Simplification of concrete measure implementation

An essential factor in the implementation of an ISMS is the capture of assets and allocation of measures to increase resilience. On the one hand, this is supported by the tool. Still, at the same time, it is also characterized by the catalogue of measures provided and the possibility of integrating further catalogues of measures. 8% of respondents rate the question about the simple measures implementation with a grade of 3, 56% with a grade of 4 and 36% with a grade of 5.

Two observations can be drawn from this: On the one hand, the developed tool optimally supports this process, and on the other hand, the catalogue of measures provided with the process model meets the requirements of the target group.

In the group with little or a maximum of 3 years of experience, only 8% of respondents give a grade of 3, compared to 75% a grade of 4 and 17% a grade of 5 (n=115).

In comparison, the picture of the group with a wealth of experience of 3 to 4 years in assessing the simplicity of implementing measures is reversed: Here, 73% rate the question with a grade of 5 and 18% with a grade of 4, only 9% of respondents award the grade 3 (n=115) (Figure 39)

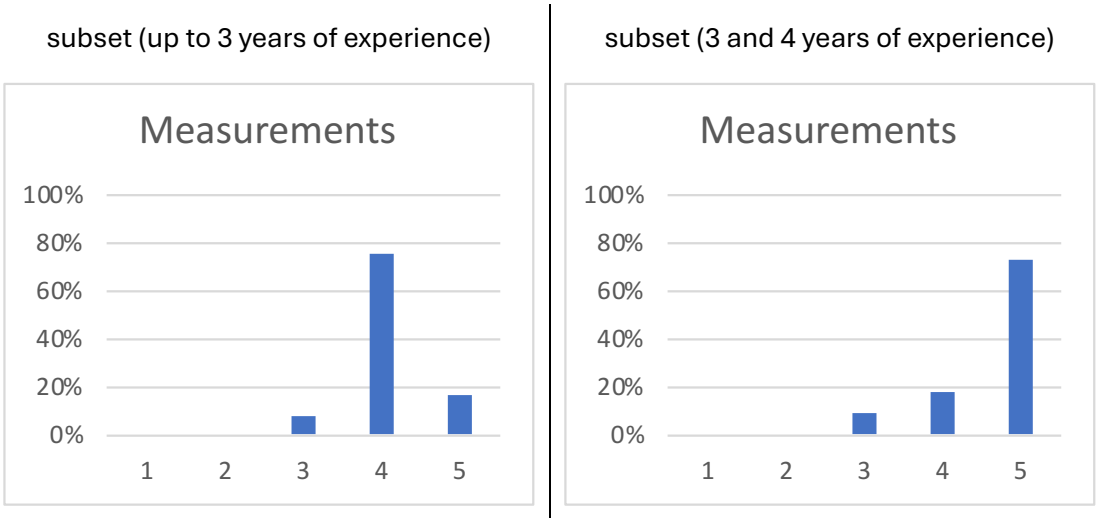

Figure 39: Simplification of the concrete measure implementation (clients form different experience groups)

Structured and comprehensible procedure model

Regarding the "Structured and comprehensible procedure model" question, both comparison groups answered approximately the same way (Figure 40). This makes it clear that the process model can be used regardless of the experience of the respective users and helps to establish the ISMS quickly and easily (Figure 40)

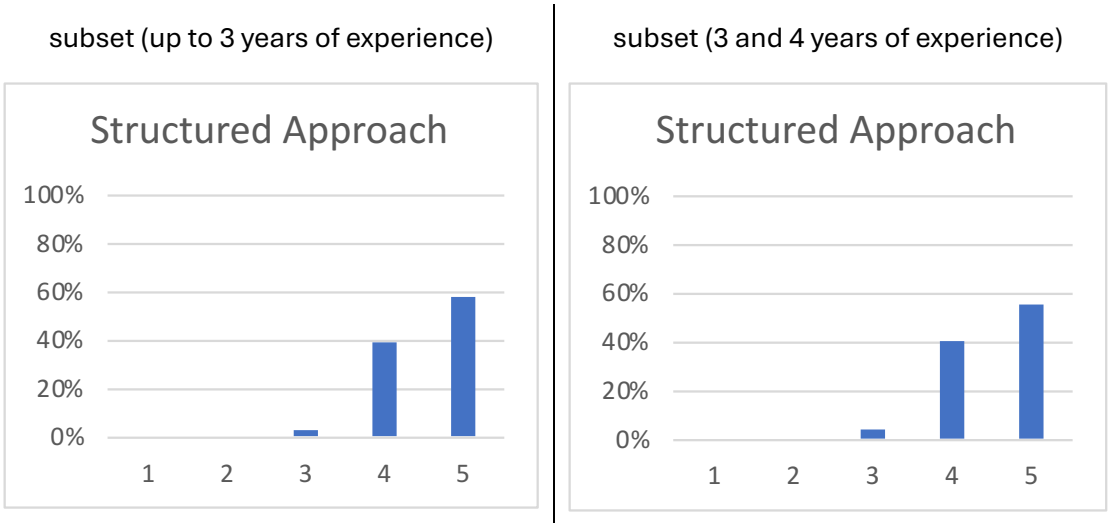

Figure 40: Structured and comprehensive procedural model (clients from different experience groups)

Implementation speed with the help of the procedure model

Since the results are approximately the same, it can also be observed when answering the question "Implementation speed with the help of the procedure model“. Of the surveyed clients who have been working with the process model for 3-4 years, 4% rate the question of the possible implementation speed with a grade of 3, 40% with a grade of 4 and 56% with a grade of 5 (n=333). In the comparison group with a maximum of 3 years of use, 7% rate this question with a grade of 3, 34% with a grade of 4 and 59% with a grade of 5 (Figure 41).

This also makes it clear that both comparison groups quickly adapt to the process model and use the advantages associated with the process model. In particular, the rapid implementation or establishment of the ISMS reduces the likelihood of failure and, at the same time, increases the chance of a sustainable establishment and strengthens the organisation's resilience against cyber-attacks.

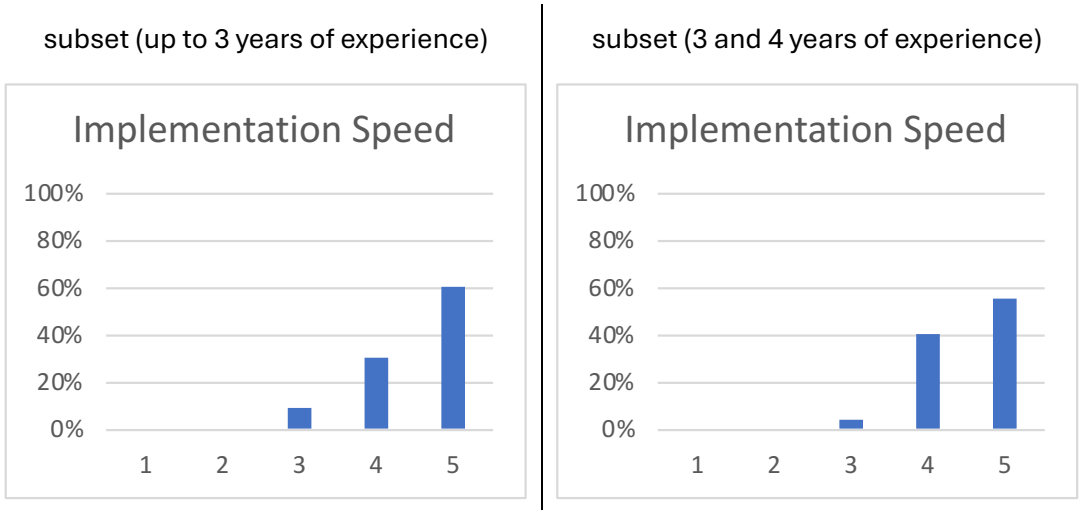

Figure 41: Implementation speed with the help of the procedural model (clients form different experience groups)

Increase the maturity of the ISMS as a KPI

The primary goal for establishing an ISMS is to increase the organisation's resilience against cyber-attacks. According to the respondents, the process model helps to increase resilience. Overall, 18% of respondents rated this with a grade of 3, 26% a grade of 4 and 56% a grade of 5 (n=333). In the group with little to a maximum of 3 years of experience, 28% rate the increase in resilience with a grade of 3, 29% with a grade of 4 and 43% with a grade of 5 (n=115). On the one hand, this can be explained by the lack of experience or usage time. On the other hand, the respective ISMS are not yet fully established, so there are no empirical values to evaluate this question. A completely different picture emerges for the group with 3-4 years of use. 79% of this group's respondents rate the resilience increase with a grade of 5. In contrast, only 20% rate the question with a grade of 4 and a negligible 1% with a grade of 3 (n=115) (Figure 42)

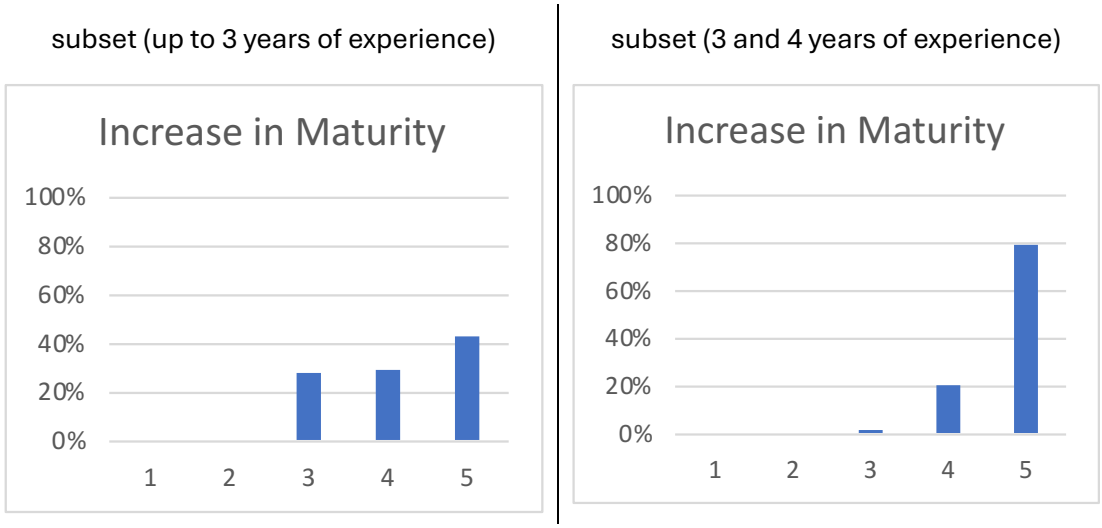

Figure 42: Increase the maturity of the ISMS as a KPI (clients from different experience groups)

Other positive side effects

All respondents reported that using the process model resulted in further positive effects at the beginning and during the establishment of the ISMS. 20% of respondents rated the synergy effects with a grade of 3, 25% with a grade of 4 and 55% with a grade of 5 (n=333). When analyzing the comparison groups, it becomes clear that these synergy effects continue to increase over time. Often, these effects only occur after the 2nd or 3rd PDCA cycle. The group with little to 3 years of experience rates this question almost equally. The group with more extended experience and possibly already certified ISMS installations evaluates the occurring synergy effects with a higher evaluation. 12% of respondents give a grade of 4, and 88% a grade of 5 (n=115) (Figure 43).

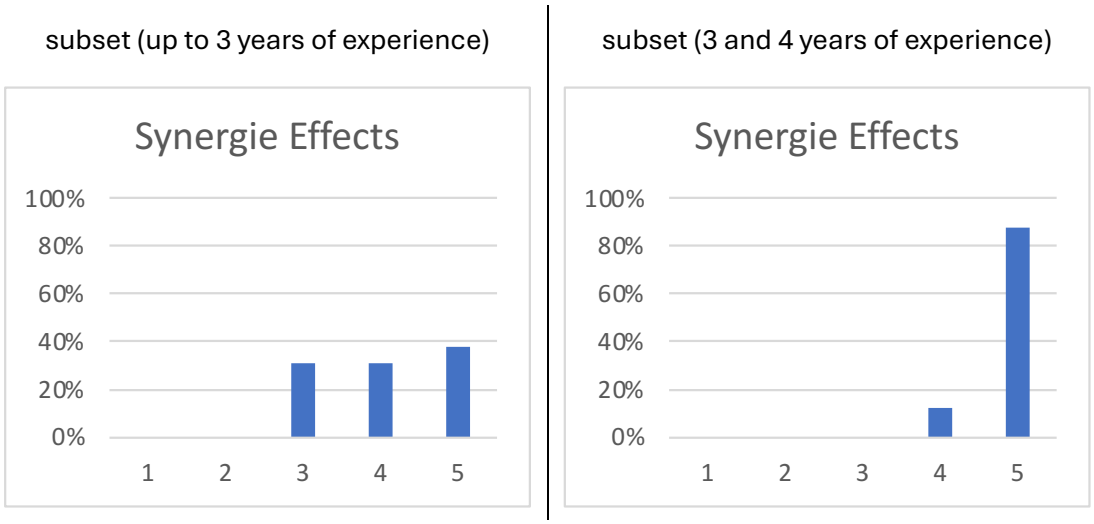

Figure 43: Other positive side effects (clients from different experience groups)

The respondents rated the evaluation questions positively throughout. Some clients have been working with the process model since 2019 and have contributed significantly to the further development of the process model with their ideas and requirements. Thus, the development, testing, and evaluation phases will be evaluated positively, and the second research question will also be answered. Of the 162 clients, all who have been working with the procedure for more than 1 year have implemented their ISMS and successfully undergone a corresponding certification.

Thus, the following results were achieved by contribution #11 for the research work:

- **Research Area**:
  - Evaluation of the process model.
- **Research Relevance**:
  - Further investigation is also outside the research domain, especially in the SME sector.
- **Research Results**:
  - The functionality and practical application of the process model could be demonstrated for the research domain.
- **Other Research Topics**:
  - Investigate whether the process model can also be used outside the research domain.

With the help of Publication #11, the research question B3 could be answered:

- **„B2. Determination of relevant activities of the process model."**
- **„B3. Development of a software prototype to support the process model."**

4.3.8 Publication #12 –CISOs as a Driver of the ISMS

In today's digital world, where data and information are valuable assets, information security is increasingly becoming a critical success factor for companies. This also applies to public administrations. To operate information security effectively and efficiently, many organizations appoint a so-called CISO (Chief Information Security Officer) as the primary person responsible for protecting data and IT systems from threats. The CISO acts as a strategic advisor, responsible not only for overseeing information security-related operations but also for helping to shape the organization's information security policies, procedures, and strategies. He also acts as a crucial bridge between the IT department and the C-suite by sharing critical information about security risks and investment needs. In addition, the CISO initiates, coordinates and monitors target group-specific training and awareness-raising measures for employees (Ciekanowski et al., 2024, p. 36).

The acronym CISO refers to an employee who holds one of the most critical roles in the organization. Its mission is to ensure a comprehensive approach to cybersecurity. The CISO supports the detection of threats, prevents their emergence and mitigates the consequences while always keeping the organization's mission in mind (Ciekanowski et al., 2024, p. 39), (Hof, 2022, p. 222f.).

As a result, organizations are increasingly recognizing the CISO as a critical element in ensuring business continuity, protecting reputation, and building customer trust through effective information security management (Ciekanowski et al., 2024, p. 36).

This recognition for the CISO is currently limited in public organizations (Meuche, 2022, p. 100), (Moses and Sandkuhl, 2024c).

A future-proof public administration is no longer conceivable without IT. At the same time, Internet threats and risks to IT infrastructures are increasing. Holistic information security management for public administrations can help to avoid or mitigate risks. Figure 44 provides an overview of the Open Security Architecture Landscape (“OSA Landscape,” 2024).

This is an overview of an organisation's various areas of responsibility in which security measures must be taken for a holistic information security management system. Usually, the CISO takes on controlling and coordinating tasks in security governance. The other areas of the OSA structure are the topics that should be considered in establishing and establishing an ISMS.

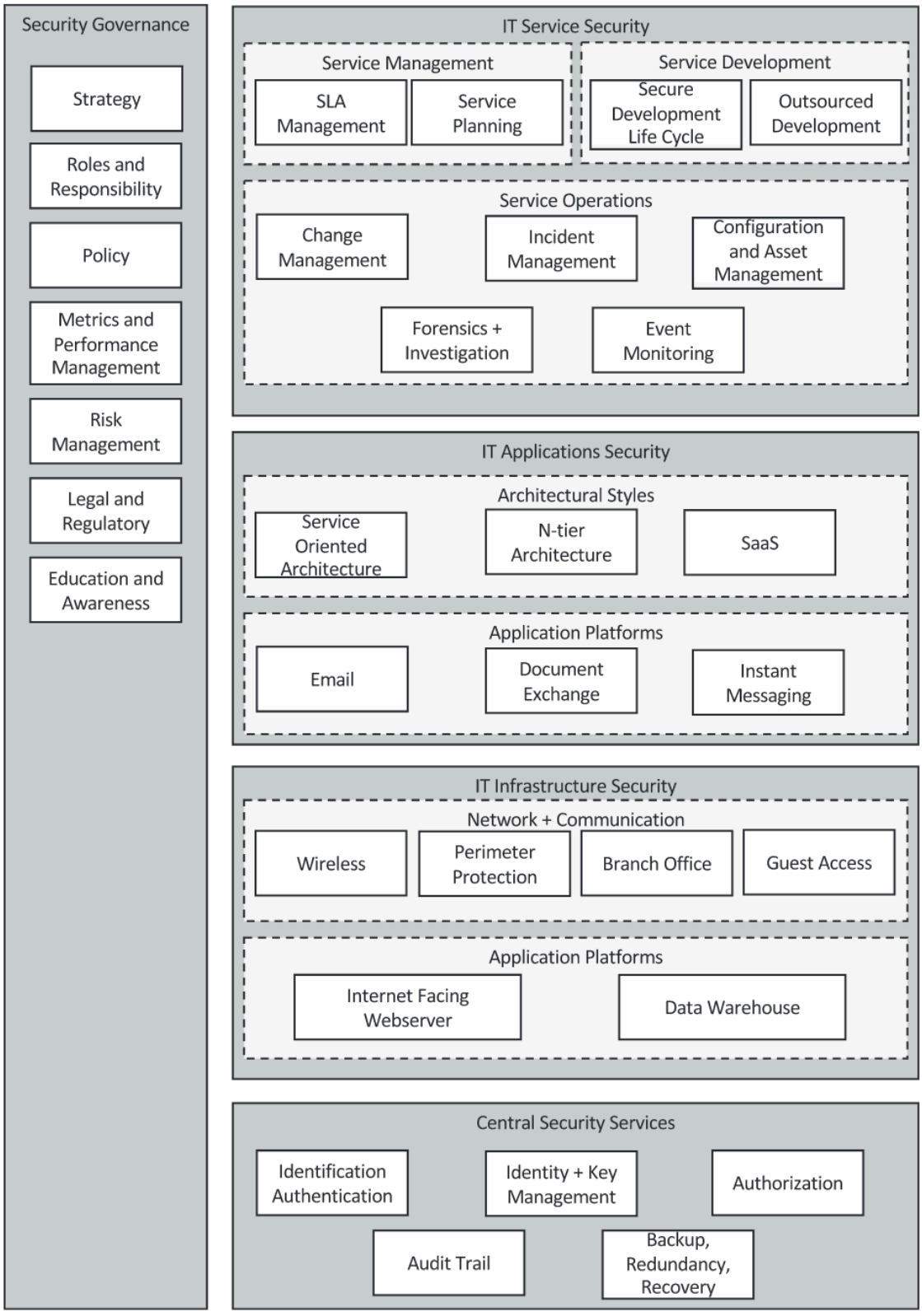

Figure 44: Open Security Architecture Landscape

Source: ("OSA Landscape," 2024)

Article #12 sheds light on the extent to which the role of the CISO is established in local governments. A study conducted with 162 participants showed that administrations place the information security officer at different hierarchical levels:

- external ISO,
- internal ISO, in line, IT department, or subordinate to it,
- internal ISO, in line with independent reporting tasks to management,
- CIO/CISO in personal union,
- CISO is a member of the C-level board.

The following Figure 45 summarises the results of the study. First and foremost, all administrations have appointed an information security officer.

Small administrations (up to 25 employees) employ external information security officers with almost 50%. As the organisation's size increases, the number of external information security officers decreases in favour of internal ones. At the same time, from an organization size of 250 employees, it can be observed that the role of the information security officer is becoming more and more important, and the information security officer is being established in a separate department or staff unit. Although the role of the CISO, unlike the data protection officer (DPO), is not provided for by law (*DSGVO*, 2021, p. Art. 37, Art. 38 and Art. 39), the importance of the CISO is increasing (Spindler, 2021, p. 40).

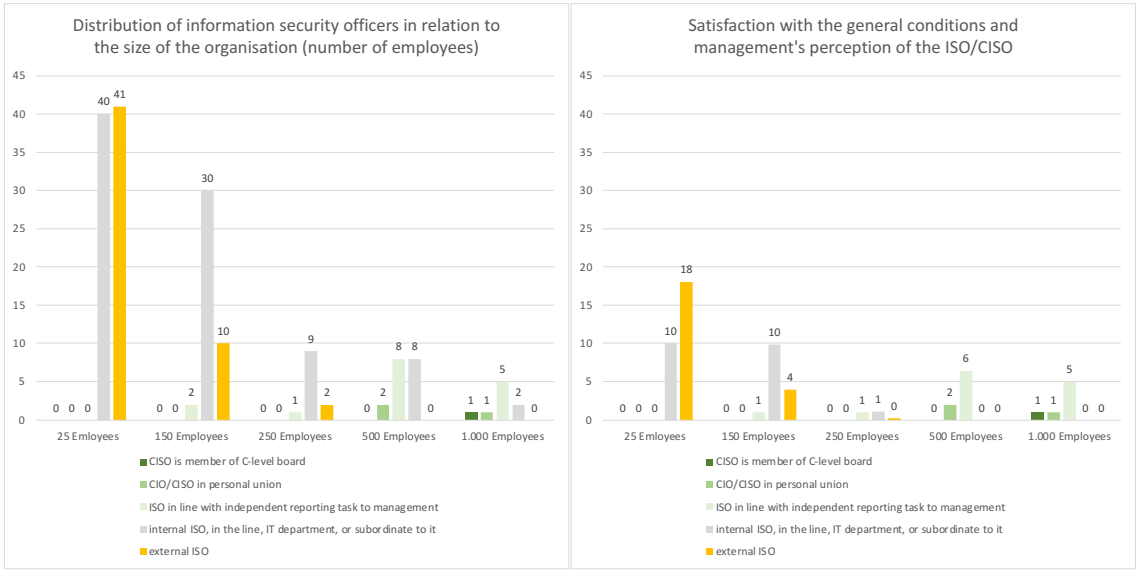

Figure 45: Distribution of ISO concerning the size of the organization and satisfaction with the general conditions and management's perception

As part of the study, the "satisfaction" of the information security officers with the framework conditions and the "perception" of the task by the management level was analyzed. As a result, 44% (= 18 of 44) of **external** information security officers from small administrations (up to 25 employees) and 40% (= 10 of 40) from medium-sized administrations (up to 150 employees) stated that they were satisfied with the framework

conditions and in particular the perception by the management level. A similar picture also prevails among **internal** information security officers. In small administrations (up to 25 employees), only 25% (=10 of 40) and in medium-sized administrations (up to 150 employees), 33% (=10 of 30) of respondents stated that they were satisfied with the framework conditions and the perception of their role by the management level. This low percentage can probably be explained by the fact that these information security officers are usually subordinate to the IT department and do not have a direct right of consultation with the management level.

The dissatisfaction of the subordinate information security officers with framework conditions and the perception of their role by the management level can be observed, especially in small administrative organizations.

This ratio only changes in larger administrative organizations (up to 500 employees or more). Without exception, the information security officers surveyed in large administrations stated that they were satisfied with the framework conditions and the management level's appreciation of their role. This is justified by the fact that the information security officer is a member of the management level or acts from a department or staff unit explicitly established for the task.

In summary, the role of the CISO as a key element of information security management is crucial in light of the growing cybersecurity threats and the increasing value of data.

The CISO is a strategic advisor overseeing information security-related operations and actively collaborates with senior management in shaping policies, procedures, and data security strategies.

Its role is not limited to the technical side of security but also includes identifying, analyzing, and managing risks and monitoring compliance with regulations and safety standards. The CISO acts as a critical communication bridge between IT and senior management by sharing crucial information about security risks and investment needs.

The conclusion is that organizations must adequately support their CISO and provide them with access to appropriate resources, including financial and human resources. This is the only way he can perform his tasks effectively (section 2.5.1). A formal designation within the framework of an ISMS project without granting corresponding rights and obligations is not expedient.

Thus, the following results were achieved by contribution #12 for the research work:

- **Research Area**:
  - CISO is the driver in ISMS matters in administrations.
- **Research Relevance**:
  - CISO is an essential Stakeholder.
- **Research Results**:
  - The CISO takes on essential tasks in the context of information security.

    - The location of the CISO in the organizational hierarchy is a critical success factor for establishing information security.
- **Other Research Topics**:
    - Increasing the importance of the CISO for small local governments.

With the help of Publication #12, the research question B3 could be answered:

- **„B2. Determination of the main stakeholder groups for consideration in the process model."**

5 Status Quo of Information Security Management in Public Administrations (Post #1)

Title	**Empirical Study on the State of Practice of Information Security Management in Local Government**
Authors	Frank Moses (frank.moses@uni-rostock) Kurt Sandkuhl (kurt.sandkuhl@uni-rostock)
Publication Body	Moses, F., Sandkuhl, K., Kemmerich, T., 2022a. Empirical Study on the State of Practice of Information Security Management in Local Government, in: Zimmermann, A., Howlett, R.J., Jain, L.C. (Eds.), Human Centred Intelligent Systems, Smart Innovation, Systems and Technologies. Springer Nature, Singapore, pp. 13–25. https://doi.org/10.1007/978-981-19-3455-1_2

Abstract

Modern administrative action is no longer conceivable without electronic communication and IT. The complexity of IT, the increasing degree of networking and the administration's dependence on IT-supported procedures have led to the fact that the security of IT and associated processes must be given high priority, and a corresponding cybersecurity strategy must be substantiated. Existing approaches either fall short or cannot be applied to the context of local government without adaptation. This article contrasts the published information security management and state-of-practice information management in governmental organizations. The empirical basis for our work are (1) audit reports of certification audits in the municipal sector, (2) expert interviews on the status quo of information security in German local government and (3) a review of scientific literature. The paper's results include current challenges in increasing the resilience of the municipal administration and open issues for future research.

Contribution to Design Science Research Step

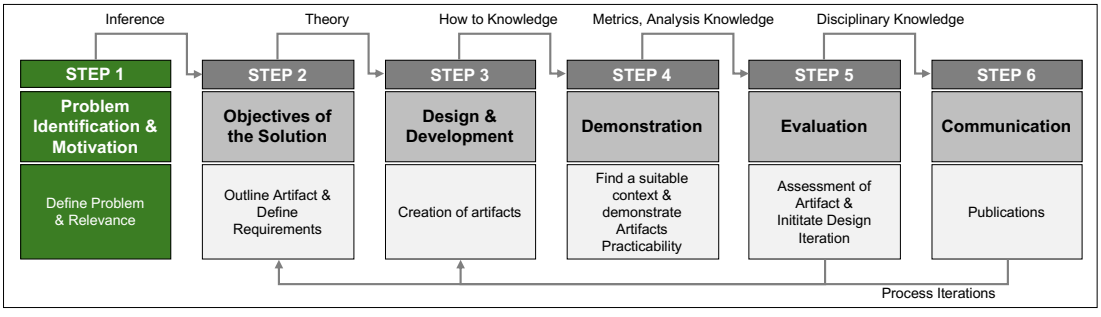

Figure 46: Publication #1 - Empirical Study on the State of Practice of Information Security Management in Local Government

5.1 Introduction

The automated processing of data and information now plays a key role in fulfilling tasks in small and medium-sized enterprises (SMEs) and local governments (Solms and Niekerk, 2013). It is a precondition for applying artificial intelligence to support human actors in such organizations and for establishing digital services and intelligent systems. To meet the societal demand for increased efficiency and flexibility of public bodies, all essential processes must be supported by information technology (IT) (Helbig et al., 2009). In addition, legal requirements such as the General Data Protection Regulation (Calder, 2018) and the E-Government Act (Heinemann, 2023) drive digitization in the respective domain forward.

Increased reliance on modern IT has significantly increased the risk of information infrastructures being adversely affected by deliberate attacks from inside and outside, negligent action, ignorance or technical failure, both qualitatively and quantitatively. Lack of information security can lead to disruptions in the performance of tasks, which can reduce the performance of authorities and, in extreme cases, bring their processes to a standstill. Furthermore, problems in information security (IS) seriously hamper the establishment of intelligent information systems, as they negatively affect the acceptance, efficiency and functionality of such systems (Kweon et al., 2021). Thus, ensuring IS is one of the central tasks of local governments; an appropriate level of security in the business processes and the associated (IT) infrastructures must be organized.

Research on information security management (ISM) has created a rich body of knowledge (cf. section 2). However, based on experiences from governmental projects, we think there is a gap between the research view on the status of ISM and the practitioners' reality. Thus, the work presented in this paper aims to contrast the state of research in ISM with the corresponding state of practice in municipalities and other governmental organizations. To address the research view, we perform a systematic literature analysis (section 2).

The empirical basis for the state of practice consists of 421 reports from IS audits carried out in the municipal sector (see section 3.1) and 42 interviews with ISM experts from German federal states and local governmental bodies (see section 3.2). Analysis of this substantial and unique material results in the identification of many challenges for the practice of ISM in local governmental organizations that so far have not been sufficiently addressed in research.

5.2 Literature Review

A structured approach was used to collect relevant literature on IS status quo in the municipal sector (Watson and Webster, 2020). A search was conducted in the literature databases SSOAR (Administrative Sciences), EBSCO EconLit and WISO (Public Service, Business Administration) and Scopus (various disciplines) with a combination of the

following search terms: "cybersecurity, public sector, information security". In addition, references to relevant systematic works from 2013 to 2021 were reviewed.

Table 14: Results of the literature review

Search query	Source	Hits	Relevance
public AND sector AND cybersecurity	Scopus	247	18
informationssicherheit		27	0
informationssicherheitsmanagement		3	1
public-sector AND cybersecurity		64	7
Public services AND information security		43	0
public AND sector AND cybersecurity	EBSCO EconLit	15	0
public-sector AND cybersecurity		1	0
cybersecurity	SSOAR	29	3
public AND sector AND cybersecurity		1	1
informationssicherheitsmanagement	WISO	9	0

The first search queries resulted in around 1,500 hits. Older literature was not considered, as publications are only relevant from 2018 due to the entry into force of the EU GDPR (Art. 32, para. 1, lit. d). The list of results was reduced to 987 titles. After a review of the titles, the abstracts of 439 papers were also read. This was followed by a review of the full text of 85 articles. When assessing their relevance based on content, quality and citation frequency, 26 papers (4 duplicates) were found relevant and included in the analysis. Table 1 summarizes the results of the search.

Table 15: Grouping after qualitative content analysis

#	Content groups	Literature
1	Validation of the technical components	(A. Weber et al., 2020), (Karsten Weber et al., 2020)
2	Analysis of factors hindering the development of cybersecurity strategies in the public sector	(Aman and Shukaili, 2021)
3	Analysis of cyber-attacks and possible preventive measures	(Ahmad et al., 2022), (Alagarsamy et al., 2021), (Kesan and Zhang, 2021), (Bouzoubaa et al., 2021)
4	Development and establishment of ISMS	(Müller, 2020)
5	Awareness Measures	(Alhashim and Rahman, 2021), (Andreasson, 2012), (Wirtz and Weyerer, 2017), (Park et al., 2017), (Alharbe, 2021), (Coppolino et al., 2018)
6	Shortage of skilled workers and effects on the public sector	(Drmola et al., 2021), (Lehto, 2020)
7	Physical Security and Security Assessment	(Phelps, 2021), (Choi et al., 2021), (Dreyling et al., 2021), (Mironeanu et al., 2021), (Savold et al., 2017)
8	Legal framework parameters in the cybersecurity domain	(Bendiek and Schallbruch, 2019; Maglaras et al., 2020)
9	Maturity Models	(Garba et al., 2020), (Zakaria et al., 2019)

In the following analysis step, the papers were assigned to the content groups in Table 2. The current research topics in the field of cybersecurity are far-reaching and mainly deal with safeguarding the technical components. Many publications shed light on the analysis of cyber attacks and possible preventive measures. It is striking that many papers focus on employees and investigate how employees' awareness of cybersecurity can be increased. Many documents describe possibilities for the protection of physical security and security assessments and discuss the shortage of skilled workers, especially in the public sector.

Furthermore, papers regarding the legal framework and digital sovereignty must be mentioned. Since the EU GDPR, IS and cybersecurity have been used increasingly synonymously and often concerning data protection and privacy issues. In contrast, only one relevant article sheds light on the structure and establishment of an ISMS.

5.3 Methodology

Various success factors influence the development and establishment of ISM systems. Interviews, case studies, and retrospective analyses are research strategies (Yin, 1981) for qualitative data collection that are well suited to present complex facts in the natural environment and to derive results from them (Eisenhardt, 1989). In the first step, audit reports from the local government domain provided by two certification bodies were analyzed. The results were used to design a questionnaire as a basis for expert interviews. The aim was to compare interview results with the results of the empirical analysis and the case studies.

5.3.1 Evaluation of audit reports

The issue of IS is not a new topic. There are corresponding concepts for developing and establishing ISM systems (“BSI-Standard 200-1,” 2024). With the help of these concepts, some local German governments have already dealt with the topic of IS and set up a management system. A structured evaluation was particularly possible in Bavaria and Saarland. Two certification bodies have allowed researchers to view and analyse audit reports. In total, 421 audit reports were analysed. The following Table 16 provides an overview of the results:

Table 16: Analysed certification audits

certification body	year	No. of Audits	passed	Passed with defects	not passed, to be repeated
IT-Sicherheits-cluster Regensburg	2019	17	0	16	1
	2020	43	0	38	5
	2021	80	0	66	14
DQS GmbH	2019	58	0	47 + 1	9
	2020	102	0	87	15
	2021	121	0	95	26
Sum		421	0	350	70

Of 421 organizations that have undergone an IS audit, no organization has achieved the goal of "passing without defects." 350 organizations passed the audit with deficiencies. For 70 organizations, however, the weaknesses identified in the audit were so significant that a so-called action plan was initiated, e.g. a reworking and elimination of the deficiencies and subsequent re-examination. One organization had not seized the opportunity to remedy the shortcomings and had not repeated the examination. All other organizations have a certificate through the audit, confirming an ISMS's successful establishment. The audit reports were examined formally (number of audits and number of passed test certificates) and materially. The following criteria were coded in advance to give the analysis more significance, and the audit reports were then qualitatively analyzed to derive core statements (Mayring, 2004, pp. 159–176).

Management Attention (Coding 1): Essential for the development of an ISM system is the assumption of the responsibility of the management level for the topic itself ("BSI-Standard 200-1," 2024). Against this background, the analysis focused on the extent to which the respective management level was involved in the ISMS process.

Leadership (Coding 2): The management initiative is essential for successfully setting up an ISMS in an organization. Nevertheless, the complex topic of ISMS requires concrete control and management tasks, which, in the best case, are taken over by the management itself or delegated accordingly and then performed.

Organizational structure (Coding 3): The planning and implementation of the security process includes defining organisational structures and roles and tasks ("BSI-Standard 200-1," 2024). With this coding, all places in the audit reports are marked, which provides information regarding organizational structure in the context of security concepts.

Process organization (Coding 4): Many organisational tasks are organized as processes, with a specific process owner, person in charge, and description. The structure of a safety system includes, in particular, the recurring processing of maintenance, incident and change processes. High-quality implementation of these processes forms the foundation of ISMS and is thus marked with code 5 in the analysis of the audit reports.

Employee Awareness (Coding 5): Recent attacks on public infrastructures have shown that a gateway is formed by the organisation's employees (Leeser, 2020). Against this background, it is interesting to find out which measures the organisations have planned and implemented concerning employee awareness.

PDCA-Cycle (Coding 6): A management system thrives on the recurring sequence of planning, implementation, review and initiation of corrective measures ("BSI-Standard 200-1," 2024). When analyzing the audit reports, great importance was attached to coding No. 6. Essentially, it is a matter of determining whether only an ISMS is being set up to obtain a one-time certificate or whether the organization operates the ISMS sustainably.

Guidelines and Documentation Task (Coding 7): Documentation is indispensable ("BSI-Standard 200-1," 2024) . An ISMS project ranges from the guideline for IS through further planning and guideline documents to clear process descriptions and verification documents. It is precisely this documentation task that poses significant challenges for small and medium-sized enterprises as well as local government. Since policy documents are to be classified in the category planning of the PDCA cycle and without a good plan, the goal is often not achieved, precisely this component of an ISMS is to be analyzed as part of the analysis of the audit reports.

Use of tools (Coding 8): Within the framework of an ISMS project, there is a need for tool support for the ISMS itself as well as for other tasks within the framework of the security concept, e.g. monitoring of network activities with the help of special tools. Tools are a critical success factor to fulfil or monitor many different tasks. Thus, statements regarding the use of tools are coded accordingly.

Implementation of measures (Coding 9): A holistic ISMS implements and plans preventive measures to remedy security incidents. When analyzing the audit reports and any existing evidence (annexes to the audit report), it is to be checked which type of measures (organizational, personnel, infrastructural and technical security measures) have been planned and implemented and what contribution they make to increasing safety.

Risk management (Coding 10): Any process or IT infrastructure operation is associated with risks. The risk management process is thus one of the foundations of a safety management system ("BSI-Standard 200-3: Risikomanagement," 2024). Experience has shown that risk identification and treatment are challenging for the municipal administration. Code 10 will be essential in analysing the audit reports to identify how risk management is embedded in the security process.

Continuous Improvement – CIP (Coding 11): To maintain IS, it must be subject to permanent improvement. Logically, this necessitates constant measurement and evaluation (*DIN ISO/IEC 27001*, 2018). How and with which results was the CIP process evaluated by the auditors in the available audit reports marked with code 11 and later assessed accordingly?

The audit reports were written by independent auditors based on the findings found during the audit. All reports have the same structure and include 20 test groups with a total of 76 test complexes. The evaluation of the test complexes was conducted based on the CMMI maturity model ("CMMI Institute - Home," n.d.). A complex of questions is considered fulfilled if it reaches at least maturity level 3. The audit is passed if no question complex with a maturity level of less than three has been assessed. Maturity level 1 is considered a serious major nonconformity, and maturity level 2 is a minor nonconformity. At maturity level 3, however, the respective test complex is considered fulfilled with considerable potential for improvement. Maturity level 4 is awarded if the respective test complex meets the essential requirements, i.e., the planning measures are completed, and the

implementation is largely completed. For a maturity level 5, the planning and implementation of a test complex must be fulfilled entirely. In addition, appropriate supporting documents must be kept. Table 15 summarizes the CMMI maturity line and its description:

Table 17: CMMI-Maturity Levels

CMMI-Maturity	Description
1	Initial: There are no specifications or documentation. Implementing measures or processes happens ad hoc and usually depends on the situation. There is no evidence. Responsibilities are not regulated. (Implementation 0%)
2	Managed: There are plans to implement the specifications. However, implementation has not yet begun. (Implementation 25%)
3	Defined: Planning measures have been completed, and implementation has begun but has not yet been fully completed. (Implementation 50%)
4	Quantitively Managed: The implementation of planned measures is underway and is nearing completion. (Implementation 75%)
5	Optimizing: Fully implemented. Written specifications are available. Evidence may be provided. Necessary processes are described, and the responsibilities are fully regulated. (Implementation 100%)

The audit reports were evaluated according to the coding and determined in which area which results were achieved by the audited organization. The result is summarized in Figure 47. It is striking that maturity levels 1-2 are strongly represented in the percentage distribution (average value 16.8%). In contrast, maturity levels 4-5 are poorly developed (average value 4.8%). Maturity level 3 has an average value of 56.8%.

When adding up the two maturity grades 1-2, coding 5, “employee-awareness” stands out in particular, with a total of 47.8%. This means that the topic of employee awareness at these institutions is suboptimal. In 2nd place is the coding 11 “CIP process” with 46.8%, closely followed by the coding 10 risk management in 3rd place with 41.8%.

This is followed in 4th and 5th place by the coding 3 organizational structure with 35.9% and coding 4 process organization with 34.9%, in 6th place the coding PDCA-cycle with 34.0%, and the 7th place the coding guidelines and other documentation tasks with 32.1%.

Finally, coding 1 management attention with 29.5% should be mentioned. These values allow the following assumptions:

- The organizations underestimated the tasks for the development and establishment of the safety management system,
- Lack of implementation experience in a security project,
- Lack of support or project expertise within the organization,
- Lack of management support for the topic,
- Missing tools, missing process models, missing best practices, etc.

These assumptions were further investigated with the help of the interview study.

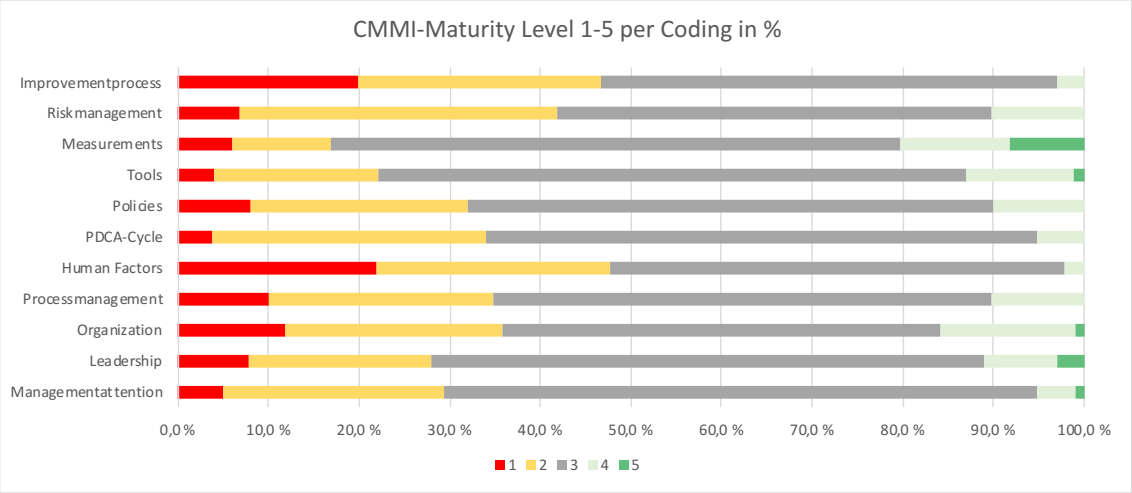

Figure 47: Results of the qualitative analysis of the audit reports

5.3.2 Interview study

A guideline-based interview study was conducted to confirm the first impressions from the analysis of the audit reports. The central research question, further defined by the interview study, is: *What are the obstacles and challenges in setting up and establishing security management systems in public administration, especially in local government?* Propositions were developed to investigate this work's central research question in the interview study. These propositions served as the basis for creating a questionnaire and, simultaneously, formed an essential input for the qualitative content analysis of the interviews.

First and foremost, the state representatives of the individual federal states and other interview partners from state, city and local governments of various German federal states were addressed. In addition, project members and responsible persons from audited organisations were considered. The survey was conducted in August and November 2021. A total of 42 interviews were conducted. The average duration of the interview was 1h:36min with 50 questions. The interviewees were confronted with open and closed questions. The obtained and transcribed results were subjected to a qualitative content analysis, according to *MAYRING* (Mayring, 2004). With the help of this method, empirical data sets can be evaluated, whereby the focus of the analysis is on understanding complex relationships. For this purpose, the relevant text passages or answers were marked and assigned to main categories and thus coded. As a result, the same texts or answers of identical main categories were summarized and resolved more finely by forming subcategories. The formation of subcategories corresponds to the induction process, which, after a catalogue-based evaluation, further defines the research question. Critical individual case interpretations have emerged as synergy effects, in addition to the category-based evaluations along the upper categories. Table 5 summarizes the assessment of the interview questions concerning the propositions.

Table 18: Overview of the interview questions vs. proposition and expectations

	Interview Questions				
Proposition	Management-attention	Lack of Employee Awareness	Need for policies	Tool-usage	Risk and Improvement
How high do you estimate the risk of your organisation becoming a cyber-attack victim?	no awareness at the management level	employee is not seen as part of the problem	possible misjudge-ment of existing risks	possible insufficient evaluation of topics	possible misjudge-ment of existing risks
Which target groups are the focus of cyber-attacks?	suppression of the topic	employee is not seen as part of the problem			no risk radar available
Have there already been concrete indications of cyber-attacks in your organization?	no statements; fear of consequences	no dependency suspected		system not implemented	
What are the distribution of roles concerning IS in the organization?	depending on success, changing the attribution of responsibility	more sporadic and not Continuous training process	no regulations desired		
What security precautions have been taken in the IT sector to protect the organization from cyber-attacks?	no involvement		lack of know-how	system not implemented	digital carelessness
What measures have been taken to protect the organization from cyber-attacks?	digital carelessness	IT is not understood as an enabler	digital carelessness	digital carelessness	lack of know-how
What are the hurdles for setting up an ISM system in the organization?	the requirement only if legally binding	more sporadic and not continuous training process	challenge is not accepted	digital carelessness	

5.3.3 Summary of results

The most crucial point of the analysis is the lack of management attention in municipal administration. The lack of awareness of the management level for the importance of IT infrastructures, their resilience, and, at the same time, their significance for the business processes of the organization has a direct negative impact on other essential framework conditions.

Management tasks, the necessary organizational structure for the safety process, and the need to create guidelines and implement documentation tasks form the basis for sustainable development and establishment of a safety management system, but on the other hand, are only rudimentarily trained or implemented.

The biggest weakness identified was the sensitization of employees to the threats from cyberspace. Existing guidelines such as the BSI essential protection are hardly used in small local governments, as both the procedure described in the guideline and the catalogue of measures with around 5.450 individual measures seem too complex and too extensive. To make matters worse, a lack of tool support in the operational areas has further negative consequences. Existing tools exceed local government requirements, require additional expertise and have no economic relationship.

5.4 Conclusion and Outlook

Research presented in this paper started from the conjecture of a gap between the state of research and state-of-practice of ISM in municipalities and local government that negatively affects digitalization efforts and hampers the implementation of intelligent digital services. The analysis of the state of practice showed substantial shortcomings and challenges in management attention, suitable organizational structures and adequate operational processes. However, these challenges did not get much attention in the literature analysed in our survey. Thus, we see clear support for our conjecture. Furthermore, there is no published research work on the state of practice with such a rich data set. This makes our analysis unique.

One of the most significant limitations of our work is the focus on the German local government regarding the data set used for the state-of-practice analysis. The conclusions drawn from this material cannot be transferred to other countries. Still, they might help to identify the focus of attention for future analysis efforts in other federal governmental structures. However, this limitation does not apply to the analysis of the state of research, i.e., we see a clear need for more research on ISM in small-scale organizations, such as SMEs or small governmental organizations.

Our results also show that the German local government is lagging the trend in terms of cybersecurity in almost all federal states. Some local governments have recognized the importance of the resilience of their IT infrastructures against the increasing cyber threat

and have already tried to establish appropriate security management systems. The analysis has shown that there is enormous pressure to act both on the part of the management level and the technical and organizational side to counteract the constantly increasing threat situation. In addition, existing process models and tools cannot be transferred to local government requirements without revision.

This article attempts to provide an overview of the obstacles and challenges and, at the same time, to lay a foundation for further research. The codes provide an analysis framework for security projects, concepts, or process models. Based on the knowledge gained, a process model for small- to medium-sized organizations is to be developed, and its function will be tested in practice by case studies.

6 Information security management in German local government (Post #3)

Title	**Information security management in German local government**
Authors	Frank Moses (frank.moses@uni-rostock) Kurt Sandkuhl (kurt.sandkuhl@uni-rostock) Thomas Kemmerich
Publication Body	Moses, F., Sandkuhl, K., Kemmerich, T., 2022b. **Information security management in German local government**. Presented at the 17th Conference on Computer Science and Intelligence Systems, pp. 183–189. https://doi.org/10.15439/2022F162

Abstract

The growing importance of information security in organizations is undisputed. This is particularly true of local governments because modern administrative action is no longer conceivable today without electronic communication media and IT procedures. The complexity of information technology, the increasing degree of networking (also with citizens) and the administration's dependence on IT-supported procedures have led to the fact that the security of information technology and associated processes must be given a higher priority, and a corresponding cybersecurity strategy must be substantiated. Existing approaches either fall short or cannot be applied to local government contexts without revision and adaptation. This article examines case studies of implementations of IT security projects in local government. The specific focus is on the differences between information security management system (ISMS) implementations of different hierarchical levels of governmental organizations. The results show current challenges in increasing the resilience of the local government.

Contribution to Design Science Research Step

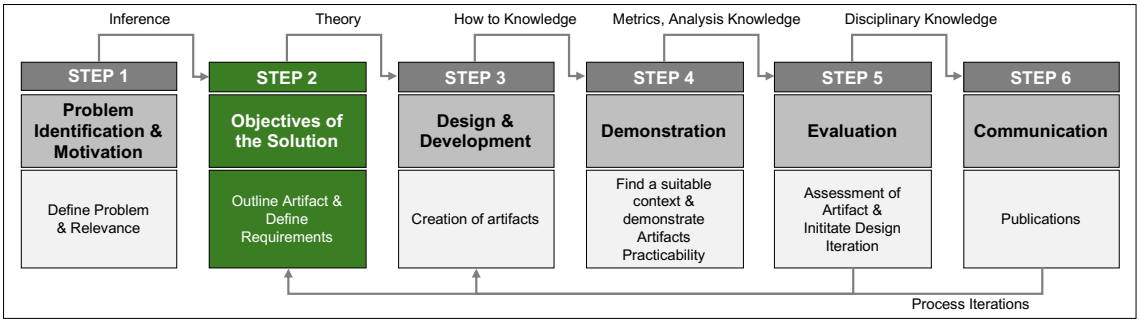

Figure 48: Publication #3 - Information security management in German local government

6.1 Introduction

Information security is a comparatively new topic in the domain of local government. The automated processing of data and information now plays a crucial role in the fulfilment of tasks in small and medium-sized enterprises (SMEs) and also in local governments (Schönbohm, 2018), (Mierowski, 2021, p. 1). All essential processes are significantly supported by information and communication technology (ICT) (Gulden, 2018, p. 137). Furthermore, legal requirements such as the General Data Protection Regulation (EU-GDPR), the Online Access Act (OZG) and the E-Government Act are driving forces of digitization in the domain (*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)*, 2022), (*OZG - Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen*, n.d.), (Heinemann, 2023)

Increased reliance on modern ICT has significantly increased the risk of information infrastructures being adversely affected by deliberate attacks from inside and outside, negligent action, ignorance or technical failure, both qualitatively and quantitatively (Leeser, 2020, pp. 86, 107), (Pohlmann, 2018, p. 196). Lack of information security can lead to disruptions in the performance of tasks, which can reduce the performance of authorities and, in extreme cases, bring their business processes to a standstill (Henseler-Unger and Hillebrand, 2018, p. 688). Against this background, ensuring information security is one of the central tasks of local governments, within the framework of which an appropriate level of security in business processes and the associated (IT) infrastructures must be organized (Kammerloher, 2021, p. 650).

This need is underlined in particular by the recent successful cyber-attacks in various federal states, especially against authorities (Gernot Heller, 2021), (Kuhn, 2021). Public authorities, in particular, are institutions of high importance for the state community. Impairments or failures may result in public service shortages, significant disruption of public security or other serious consequences (BSI, 2021). A case study analysis was carried out to study the information security of local governments. The work described here aims to identify the state of information security of local governments and critical public infrastructures to contribute to the research field of information security in the domain of local government. The specific focus is on the differences between information security management system (ISMS) implementations of different hierarchical levels of governmental organizations.

6.2 Research Method

The work presented in this paper is part of a PhD project aiming at methodological and technological support for information security management that is tailored to the needs of small and medium-sized local government units. The PhD project follows the paradigm of design science research (Hevner et al., 2004) and starts with an analysis of (a) existing scientific work in the field of information security management (ISM) for local governments and (b) an analysis of typical problems in local government's ISM as visible in information security audit reports. The detailed results of both steps are available in (Moses et al., 2022a); the literature analysis is summarized in section 3.

As the audit reports analyzed in (b) mainly reflected ISM implementations' shortcomings, we also decided to look for successful elements of ISM implementations by analyzing ISM cases. This paper focuses on these cases that – in a DSR context - contribute to investigating problem relevance and requirements for the envisioned artefact. The research question for this work is: What are the differences (if any) between ISMS implementations of different kinds and hierarchical levels of governmental organizations?

The introduction of information security management systems (ISM) usually represents an intervention in existing business processes and is influenced by various success factors. Case studies and retrospective analyses are research strategies (Yin, 1981) for qualitative data collection, which are very well suited to investigate complex issues in the natural environment (Eisenhardt, 1989). Qualitative data analysis methods help to understand process sequences and the dynamics of concrete situations under certain framework conditions and to derive results from them (Wilde and Hess, 2006).

Thus, we analyzed various ISM cases. Although our cases show many characteristics of qualitative case studies as described by (Yin, 1981) (e.g., defined boundaries, defined research question, rich set of qualitative material, etc.), we prefer the term "ISM case" because most of the case material was not collected with the case study research method in mind but evaluated ex-post as case material. Here, the eXperience methodology (Schubert and Bhaskaran, 2007) supports the research work on the one hand in the uniform preparation of the ISM cases and on the other hand, it can be ensured that the ISM cases are made comparable to derive concrete results from them.

6.3 Summary of Literature Analysis

To identify relevant literature on the status of ISM in the local government sector, a structured literature search was carried out following (*EGovG - Gesetz zur Förderung der elektronischen Verwaltung*, n.d.). The literature search was conducted in the databases EBSCO EconLit and WISO (Public Service, Business Administration), SSOAR (Administrative Sciences) and Scopus (various scientific disciplines) with a combination of

the search terms: "cybersecurity, public sector, information security". In addition, references to relevant systematic works from 2013 to 2021 were reviewed.

The initial search resulted in more than 1,500 hits, which were reduced to 85 articles in several steps by examining the titles, keywords and abstract. It followed an assessment of their relevance using the content, quality, and citation frequency. Finally, 26 papers were classified as relevant and grouped into thematic areas. Table 19 shows these areas and the appropriate papers.

Table 19: Relevant Literature sorted by thematic areas

Thematic area	Literature
Validation of technical components	(A. Weber et al., 2020), (Karsten Weber et al., 2020)
Analysis of factors hindering the development of cybersecurity strategies in the public sector	(Aman and Shukaili, 2021)
Analysis of cyber-attacks and preventive measures	(Ahmad et al., 2022), (Alagarsamy et al., 2021), (Kesan and Zhang, 2021), (Bouzoubaa et al., 2021)
Development and establishment of ISMS	(Müller, 2020)
Awareness measures	(Alhashim and Rahman, 2021), (Andreasson et al., 2021), (Wirtz and Weyerer, 2017), (Park et al., 2017), (Alharbe, 2021), (Coppolino et al., 2018)
Lack of skilled workers in the public sector and its effects	(Drmola et al., 2021), (Lehto, 2020)
Physical Security and Security Assessment	(Phelps, 2021), (Choi et al., 2021), (Dreyling et al., 2021), (Mironeanu et al., 2021), (Savold et al., 2017)
Legal Framework parameters in the cybersecurity domain	(Bendiek and Schallbruch, 2019; Maglaras et al., 2020),
Maturity models	(Garba et al., 2020), (Zakaria et al., 2019)

Most papers deal with safeguarding the technical components or tackling the analysis of cyber-attacks and possible preventive measures. It is striking that many papers focus on the staff and examine how their awareness of cybersecurity can be increased.

Also, a substantial number of papers address options for protecting physical security and security assessments and discuss the lack of skilled workers in the public sector.

Furthermore, papers regarding the legal framework and digital sovereignty must be mentioned.

Since the introduction of the EU-GDPR in 2018, information and cybersecurity have been used increasingly synonymously and often with data protection and data protection issues. In contrast, only one relevant article addresses the structure and establishment of ISM systems.

6.4 ISM Cases

Although the topic of information security in local government has only recently been given more attention in Germany, corresponding concepts for the development and establishment of information security management systems already exist (“BSI-Standard 200-1,” 2024), (*DIN ISO/IEC 27001*, 2018). With the support of these concepts, a few local governments have already dealt with information security and set up a corresponding management system. The municipalities examined in the focus of this research are mainly in the two federal states of Germany, namely Bavaria and Saarland. These organizations are motivated by funding programs of the respective state government to introduce and operate a corresponding security management system.

6.5 Case material

One of the authors supervises various institutions in setting up information security management systems to increase the resiliency of the respective organizations. The associated ISM cases were conducted from 2018 to 2022 and cover a wide range of state, city and local governments, an SME, and a critical infrastructure from four federal states. Various municipal organizations throughout Germany were asked to participate in the ISM cases. In addition, further municipal case study participants from other federal states without a funding program and three medium-sized companies were sought as a comparison group willing to have the development of their information security management system scientifically accompanied. The cases consist of local governments (small to medium-sized), district council offices, city administrations, state companies, state administration and a company, and a hospital network. For this contribution, 24 ISM cases that exemplify the situation in the German local government were selected.

Table 20: ISM Analysed Cases

#	Governmental Organization	Federal State	Type of organization
1	Gemeinde ****dorf	BY	Local government
2	Gemeinde Ma******	SL	Local government
3	Gemeinde Post*****-****	BY	Local government
4	Landeshauptkasse Saarland	SL	State administration
5	Zentrales Travelmanagement Saarland	SL	State administration
6	Landratsamt Frei****	BY	District Office
7	Landratsamt Neu*****	BY	District Office
8	LEG-Service GmbH	SL	Enterprise
9	Markt ***bach	BY	Local government
10	Markt ******dorf	BY	Local government
11	Performa Nord GmbH	HB	Enterprise
12	SlyCon GmbH	SL	SME
13	Stadt Hi****	NW	Municipality
14	Stadt ***heim	BY	Municipality
15	Stadt Neuburg a.d. Donau	BY	Municipality
16	Stadt *******furt	BY	Municipality
17	Stadt S*****fen	BY	Municipality

18	Stadt St. *******	SL	Municipality
19	Stadt ****bach	SL	Municipality
20	Stadt *******hausen	BY	Municipality
21	Stadtwerke *******hausen	BY	Municipal Utilities (critical)
22	Stadt *****burg	BY	Municipality
23	VG Neumarkt i.d. Oberpfalz	BY	Local government
24	VG ****beuren	BY	Local government

In all ISM cases, the documentation of ISMS, including organization structure and processes, was available and analysed. Furthermore, access to the stakeholders in the organization made it possible to collect required information from other reports. This was used during ISM case analysis.

6.6 Coding for Cross-Case Analysis

The cases listed in the previous section cover different hierarchical levels of local government and also other IT security areas. The case analysis aimed to identify patterns, similarities, and differences in the cases, which allowed conclusions to be drawn about generally valid relationships, proven process models, and framework conditions.

The case material was examined. To give the analysis more significance, the following criteria were coded in advance according to *MAYRING* (Mayring, 2015), followed by a content analysis of the case material so that corresponding core statements could be derived. The following describes the coding.

Table 21: Coding Scheme for the qualitative content analysis of the ISM cases

#	Coding
1	Management Attention
2	Leadership
3	Organizational structure
4	Process organization
5	Employee awareness
6	PDCA-Cycle
7	Guidelines and other documentation tasks
8	Use of tools (ISMS tools, control tools, etc.)
9	Implementation of measures (Increased IT security)
10	Risk management
11	CIP process (Assessment and measurement)

Management attention (Coding 1): Essential for the development of an information security management system is the assumption of the responsibility of the management level for the topic per se (“BSI-Standard 200-1,” 2024, p. 7), (Pfeiffer, 2022, pp. 24–27). Against this background, the analysis focused on the extent to which the respective management level was involved in the ISMS process.

Leadership (Coding 2): The management initiative is essential for successfully setting up an ISMS in an organization. Nevertheless, the complex topic of ISMS requires concrete

control and management tasks, which, in the best case, are taken over by the management itself or delegated accordingly and then performed.

Organizational structure (Coding 3): The planning and implementation of the security process includes the definition of organizational structures and the definition of roles and tasks (“BSI-Standard 200-1,” 2024, p. 28). With this coding, all places in the ISM cases are marked, which provides information regarding the organizational structure in the context of the security concept.

Process organization (Coding 4): Many organisational tasks are organized as processes, with a specific process owner, a person in charge, and a description. The structure of a security management system includes, in particular, the recurring processing of maintenance, fault and change processes. The qualitative implementation of these processes forms the foundation of an ISMS and is therefore marked with code 4.

Employee awareness (Coding 5): Recent attacks on public infrastructures have especially shown that the organisation's employees form a gateway (Leeser, 2020, p. 54). And these must be sensitized accordingly (Meuche, 2022). Against this background, it is interesting to find out which measures the organisations have planned and implemented concerning employee awareness.

PDCA-Cycle (Cycle 6): A management system thrives on the recurring sequence of planning, implementation, review and initiation of corrective measures (“BSI-Standard 200-1,” 2024, p. 17). In the analysis of the ISM cases, great emphasis was placed on coding No. 6. Essentially, it is a matter of determining whether only an ISMS is being set up to obtain a one-time certificate or whether the organization operates the ISMS sustainably.

Guidelines and Documentation task (Coding 7): The documentation task is indispensable (“BSI-Standard 200-1,” 2024, p. 21) and in an ISMS project, ranges from the guideline for information security through further planning and guideline documents to clear process descriptions and verification documents. It is precisely this documentation task that poses significant challenges for small and medium-sized enterprises as well as for local governments. Policy documents belong to the PDCA cycle planning category, and the goal is often not achieved without a good plan. Therefore, as part of the analysis of the ISM cases, this component of an ISMS will be analyzed in detail.

Use of tools (Coding 8): Within the framework of an ISMS project, there is a need for tool support for the ISMS as well as for other tasks within the framework of the security concept, e.g. monitoring of network activities with the help of special tools. Tools use is a critical success factor in fulfilling or monitoring many different tasks. Against this background, statements regarding the use of tools are coded accordingly.

Implementation of measures (Coding 9): A holistic ISMS implements and plans preventive measures to remedy security incidents. When analyzing the ISM cases, examining which type of measures (organizational, personnel, infrastructural, and

technical security measures) have been planned and implemented and what contributions they make to increasing security is crucial.

Risk management (Coding 10): Any process or IT infrastructure operation is associated with risks. The risk management process is thus one of the foundations of a security management system ("BSI-Standard 200-3: Risikomanagement," 2024, p. 7). Experience has shown that risk identification and treatment are particularly difficult for local governments. To identify how risk management is embedded in the security process, Coding 10 will play an essential role in analysing the ISM cases.

Continuous improvement - CIP (Coding 11): To maintain information security, it must be subject to permanent improvement. Logically, this necessitates continuous measurement and, above all, evaluation. (*DIN ISO/IEC 27001*, 2018). How and with which results was the CIP process implemented in the respective ISM cases marked with code 11 and later evaluated accordingly?

6.7 Case Analysis

6.7.1 Groups of Cases and Their Difference

Based on the coding and analysis of the available case material, groups of governmental organizations were identified and differences in their ISM implementations were recognized. These groups are summarized in the following.

Local Government cases – Adoption and Diffusion of an ISMS

The eight ISM cases from the domain of local government essentially address the challenges of setting up and establishing an information security management system in a small administrative organization (max. 25 employees). At the same time, these "small" local governments have to meet the increased demands on administrative processes due to increasing digitization. Furthermore, due to the tight tariff structure of public service, organizations are often unable to engage employees with the appropriate qualifications. In addition to IT technology, both internal and cross-organizational challenges have been identified that must be solved for successful implementation. Furthermore, the documentation task is one of the biggest challenges small local governments face. In addition, there is a lack of suitable tools that support developing and establishing this target group's information security management system.

District Administration cases – Implementation of the Security Requirement

A different picture emerges in the case of the two ISM cases from the domain of district administration. The necessary human and financial resources are available here. Nevertheless, additional tasks must be performed within this domain, which is needed as

a service for the subordinate administrative levels. The ISM cases focused on the challenges that arise from developing an information security management system in organizations. In large administrative organizations, the management attention, role definition, and process descriptions, especially in the IT and security domain, are suboptimal. Due to hierarchical levels within parts of a wide lead span, losses occur at the organizational interfaces (structure and process organization). Furthermore, the involvement of stakeholders and their training and sensitization, as well as employees, for the requirements of information security is a significant challenge.

City Administration cases – Security in Organizational Processes

The eight city administrations have to cope with different challenges in terms of IT security compared to other municipal organizations. Processing sensitive (often private) data requires a particularly secure handling of this data. Based on the introduced information security management system, the established strategy is supplemented by modern measures for data backup and process automation. Furthermore, the maturity level derived from the information security management system can be used to obtain data that can be used to support further management decisions. For example, it can be used to secure make-it or buy-it choices that aim to outsource certain services, both for economic and security reasons. Furthermore, this strategy replaces the heterogeneous risk landscape in favour of new uniform risk assessments. Using suitable tools to support the ISMS process was essential in these ISM cases.

State Administration cases – Secure Business Processes for Financial and Travel Transactions

The ISM cases use the example of "state accounting" and central travel management to describe the challenges there in the context of IT security. In addition to the administration of a large amount of private data within the scope of the tasks of the travel management process, the business process of "state accounting", in particular, forms a core process of a state administration. In this process, all bookings of a state administration converge. Many interfaces (e.g., with banks, debtors and creditors) must be secured organizationally, contractually and technically. The information security management system, which has been established in the meantime, forms the foundation for further strategies to guarantee information security, especially in payment transactions and travel management. This is based on advanced risk management, which provides a dashboard that aggregates and provides data from different sources. The C-Level Management is now in a position to identify and treat aggregated risks that were previously not the focus of implementing measures as individual risks.

National Company case – IT Security at an Airport Operator

The main focus of the ISM case at an airport operator is the reactions to the ransomware attack that took place there in the autumn of 2020. This attack has given the impetus to implement planned measures more quickly.

At the same time, the attack and the associated ransom demand have increased the management's attention accordingly. As a result, both human and financial resources were made available to build up the non-existent risk management and to promote the implementation of measures to increase IT security.

The forensic analysis revealed that a lack of employee sensitization and training and, partly, organizational failure were the main causes of the successful cyberattack. As a result, the following points can be mentioned to better defend against targeted attacks on critical infrastructure in the future:

- Implementation of a sustainable organization-wide IT security concept,
- Streamline the threat detection process and
- Increase in the ability to deal with threats,
- Further establishment of an open cooperation of all those responsible and
- Use of suitable tools (e.g. monitoring PDCA cycle, risk and maturity model)

Clinic Network case – IT Security at a Hospital Network and Municipal Utilities

Another ISM case was carried out in a clinic network. German hospitals, as part of the public critical infrastructure, are motivated on the one hand by various successful cyber-attacks against hospital infrastructures, on the other hand by legal requirements to introduce an information security management system (Studier and epubli GmbH, 2021, p. 196). The central topic of the ISM case in the hospital network and the critical infrastructure of the municipal utilities examined is the use of suitable tools that accompany and optimize the introduction and implementation of an information security management system taking into account different standards (e.g. BSI Compendium 2022 and the B3S[4] of the German Hospital Association).

6.7.2 Application of Coding Scheme

Using the coding presented in Table 21, all ISM cases were examined concerning the maturity the individual case showed for the aspect represented by the coding. The maturity levels were from level 1 (low maturity – only basic implementation) to level 5 (high maturity - managed and optimized status). All ISM cases focused on introducing an information security management system to increase the resiliency against cyber-attacks of the respective organization.

[4]B3S – Branch-Specific Security Standard

As part of the ISM cases, a prototypical process model developed by one of the authors was used (Moses and Rehbohm, 2022a, p. 61ff). This process model attempts to eliminate the shortcomings revealed in the audit reports' analysis. In essence, a positive result was achieved for all facilities. Some of the organizations mentioned above have already successfully passed an audit; others are still working towards it.

An analysis of the audit reports of the subjects from the ISM cases and the ISM cases themselves showed a significant improvement in the individual codes. Thus, a substantial improvement in the maturity level of the information security management system and organizational resilience can be observed. The results can be found in Table 22.

Table 22: Distribution of Maturity Levels in the ISM Cases for the different Codings[5]

	Distribution of encodings in %				
Coding	1	2	3	4	5
1	4,2	8,3	58,3	20,8	8,3
2	4,2	8,3	66,7	12,5	8,3
3	0,0	12,5	75,0	8,3	4,2
4	8,3	20,8	50,0	16,7	4,2
5	4,2	8,3	45,8	29,2	12,5
6	4,2	20,8	41,7	29,2	4,2
7	0,0	4,2	37,5	54,2	4,2
8	0,0	0,0	20,8	75,0	4,2
9	0,0	0,0	41,7	50,0	8,3
10	4,2	20,8	54,2	16,7	4,2
11	8,3	8,3	62,5	16,7	4,2

6.8 Summary and Discussion

24 ISM cases were carried out, which qualitatively examined projects to increase IT security, IT security concepts or individual IT security measures of different levels of German local governments from four federal states.

A prototypical procedure was used for the supported organizations, which enables them to implement corresponding projects to ensure information security in a practicable way. At the same time, a basis was created for incorporating the findings made in the preliminary analysis into the process model. As a result, the respective organization is supported organizationally, technically, and structurally.

To identify patterns in the ISM case series, a cross-case analysis in the form of qualitative content analysis, according to *MAYRING,* was carried out after the completion of the projects. This was also applied to secure the process model in a domain outside the local government. The results obtained confirm the findings from the primary research domain.

[5]Values are rounded to one decimal place.

This article contributes to understanding the overall context of successful IT security projects for implementing IT security concepts in local government. For the present work, the methodological limitations of case studies apply. Nevertheless, the generalizability of the results is possible, as shown by the comparison group with three companies.

Further research will show whether qualitative and quantitative research based on this confirms the similarities and differences found.

One of the most significant limitations of our work is the focus on German local governments. The conclusions derived from this material cannot be transferred to other countries. Still, they might help to identify the focus of attention for future analysis efforts in other federal governmental structures. However, this limitation does not apply to the analysis of the state of research, i.e., we see a clear need for more research on ISM in small and medium-sized governmental units.

7 Adoption and Diffusion of an ISMS with CISIS12 (Post #4)

Title	**Adoption and Diffusion of an ISMS with CISIS12**
Authors	Frank Moses (frank.moses@uni-rostock) Kurt Sandkuhl (kurt.sandkuhl@uni-rostock)
Publication Body	Moses, F., Sandkuhl, K., 2022a. Mit CISIS12 ein ISMS aufbauen. Datenschutz Datensicherheit DuD 46, 654–659. https://doi.org/10.1007/s11623-022-1677-5

Abstract

The recent cyber-attacks, including on municipal infrastructures, make it clear that municipalities must also set up an information security management system (ISMS). This is because the administration provides its own services and ensures that citizens' data is adequately protected based on legal requirements. As an easy-to-use process model, CISIS12 offers the opportunity to set up and sustainably operate a compliance and security management system in 12 steps in local governments as well as in the SME sector, thus increasing cyber resilience in the respective organization.

Contribution to Design Science Research Step

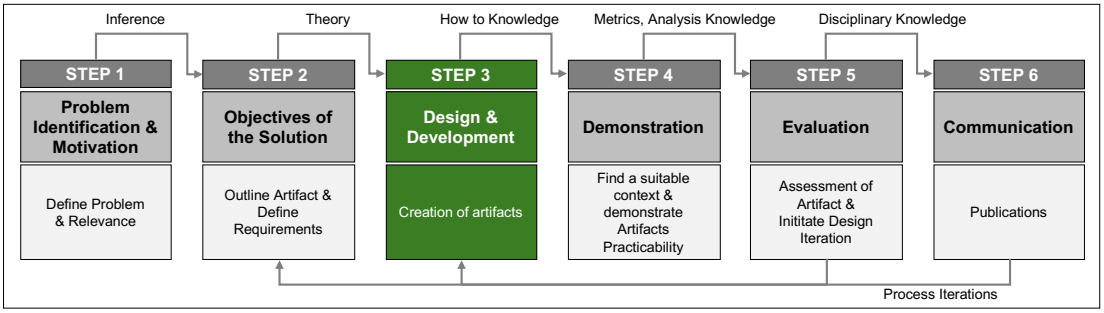

Figure 49: Publication #4 - Adoption and Diffusion of an ISMS with CISIS12

7.1 Introduction

The automated processing of information (Schönbohm, 2018, p. 429) and data (Mierowski, 2021, p. 1) now plays a vital role in the fulfilment of tasks in local governments and small and medium-sized organisations (SMEs). All essential processes are significantly supported by information and communication technology (ICT) (Gulden, 2018, p. 137). The complexity of information technology, the increasing degree of networking, and the dependence on IT-supported processes require that the security of information technology become increasingly important. On the other hand, legal requirements such as the EU Directive on Network and Information Security (NIS2 Directive), the General Data Protection Regulation (GDPR), the Online Access Act (OZG) and the E-Government Act continue to advance digitalisation in local government. The increased reliance on modern ICT has significantly increased the risk of information infrastructures being compromised by deliberate attacks from outside and domestic, negligence, ignorance or technical failure, both qualitatively and quantitatively (Leeser, 2020, pp. 86, 107), (Pohlmann, 2018, p. 196). Lack of information security can lead to disruptions in the performance of tasks, reduce the performance of authorities, and, in extreme cases, bring their business processes to a standstill (Henseler-Unger and Hillebrand, 2018, p. 688). Against this background, ensuring information security is one of the central tasks of local governments, within which an appropriate level of security must be organized in the business processes and the associated (IT) infrastructures (Kammerloher, 2021, p. 650). This necessity is underlined particularly by the recent successful cyberattacks in various federal states, especially on public authorities (Gernot Heller, 2021), (Kuhn, 2021). Disruptions or failures may result in shortages of public services, significant disruption of public safety or other serious consequences (BSI, 2021).

This article presents a corresponding process model for developing and establishing an information security management system.

7.2 State of research and literature

The number of research projects in the cyber and information security field is growing steadily, focusing mainly on the area of critical IT infrastructures (Schallbruch, 2017). *KIPKER* provides a comprehensive presentation of IT security law, including the technical basics (Kipker, 2020). On the other hand, some works postulate the required digital transformation of the public sector but only marginally shed light on information security (Bär et al., 2018). *BOSTELMANN* describes the security strategies of the German government and the EU and sheds light on the abovementioned laws and guidelines. The result of his analysis is that the municipalities are addressed as bearing the main burden in implementing the OZG (Bostelmann, 2021, pp. 183, 188). Specific instructions for action are limited to a handout for creating an information security policy. However, concrete implementation instructions for developing and establishing an ISMS remain open. However, implementation guidelines

can be found in the literature, mainly for the SME sector. Literature in this area includes a comprehensive presentation of information security challenges while considering data protection requirements (Hanschke, 2020a).

SCHÜNEMANN also acknowledges cybersecurity's particular relevance in digitalization and sees the state and administration as having a creative obligation to guarantee the functioning of their IT systems that are worthy of protection. However, developing information security frameworks can only be one component of future cybersecurity (Klenk et al., 2020, p. 3).

Without organisational and technical measures, many business processes can no longer be protected against cyber-attacks or other manipulations (Hohmeister and Rückel, 2021). This requires a higher-level management system that can be used to drive forward the development and establishment of an ISMS and its control and optimization (Sowa, 2017, p. 18). Experience from implementing other management systems has shown that IT-supported tools help support information management and process support. A tool suitable for the domain as a flank could, therefore, positively influence the security process. The relevant literature mainly sheds light on higher-level management systems. They all have in common that no concrete recommendations for action, process models or best practices for implementing an ISMS project in local government are described. This is where this article comes in.

The authors have already published a summary of further relevant literature on the subject of research (Moses et al., 2022a).

7.3 Methodological Approach

The introduction of IT security management systems usually represents an intervention in existing business processes and is influenced by various success factors. Case studies (Yin, 1981) and retrospective analyses represent research strategies for qualitative data collection, which are very well suited to investigate the complex issues to be considered in the natural environment (Eisenhardt, 1989). Qualitative data analysis methods are an essential tool for understanding process flows and the dynamics of concrete situations under certain conditions and derive results from them (Wilde and Hess, 2006).

In the first step, audit reports provided by independent certification bodies were analysed, and concrete case studies for the development of an ISMS were accompanied. On the one hand, the eXperience (Schubert and Bhaskaran, 2007, p. 16) methodology supported the research process in the uniform creation of the case studies. It thus ensured the comparability of the case studies. The audit reports, and case studies were examined both formally and substantively (Moses et al., 2022a). To make the analysis more meaningful, the following criteria were defined in advance according to *MAYRING* (Table 23) and used in the

qualitative content analysis to code the audit reports and case studies to derive corresponding key messages (Mayring, 2015).

Table 23: Coding Table

Nr	Coding
1	Management Attention (Pfeiffer, 2022)
2	Leading Tasks
3	Organisational Structure
4	Process Organisation
5	Employee awareness (Leeser, 2020), (Meuche, 2022)
6	PDCA-Cycle
7	Guidelines and other documentation
8	Use of tools
9	Implementation of measures
10	Risk management
11	Continuous improvement process (CIP)

The results of the evaluation of the audit reports about the analysis mentioned above criteria are in Table 24 below, following the maturity levels defined in CMMI (Hertneck and Kneuper, 2012). In CMMI, maturity level 1 means low maturity (e.g. no fixed processes or structures), while 5 denotes optimum ripeness.

Table 24: Results of the qualitative Analysis of the Audit reports

		CMMI-Maturity Level in %				
Coding	with/without Prototype	1	2	3	4	5
1	without	5,0	24,5	65,3	4,3	1,0
	with	4,2	8,3	58,3	20,8	8,3
2	without	7,8	20,2	61,0	8,1	2,9
	with	4,2	8,3	66,7	12,5	8,3
3	without	11,9	24,0	48,2	15,0	1,0
	with	0,0	12,5	75,0	8,3	4,2
4	without	10,0	24,9	54,9	10,2	0,0
	with	8,3	20,8	50,0	16,7	4,2
5	without	21,9	25,9	50,1	2,1	0,0
	with	4,2	8,3	45,8	29,2	12,5
6	without	3,8	30,2	60,8	5,2	0,0
	with	4,2	20,8	41,7	29,2	4,2
7	without	8,1	24,0	58,0	10,0	0,0
	with	0,0	4,2	37,5	54,2	4,2
8	without	4,0	18,1	64,8	11,9	1,2
	with	0,0	0,0	20,8	75,0	4,2
9	without	5,9	10,9	62,9	12,1	8,1
	with	0,0	0,0	41,7	50,0	8,3
10	without	6,9	34,9	48,0	10,2	0,0
	with	4,2	20,8	54,2	16,7	4,2
11	without	20,0	26,8	50,4	2,9	0,0
	with	8,3	8,3	62,5	16,7	4,2

Note: Values are rounded to one decimal place.

It is striking that maturity levels 4-5 are weakly developed in the percentage distribution (mean value 4.8%). On the other hand, maturity levels 1-2 are strongly represented (mean value 16.8%). Maturity level 3 has an average value of 56.8%. In the maturity levels 1-2,

employee awareness (No. 5) stands out in particular, with a total of 47.8%. This means that the topic of employee sensitization is poorly developed at the institutions examined.

In 2nd place is the No. 11 CIP process (assessment and measurement), with 46.8%, closely followed by No. 10 Risk Management, which is in 3rd place at 41.8%. This is followed in 4th and 5th place by No. 3 Organizational Structure with 35.9% and No. 4 Process Organization with 34.9%, in 6th place the PDCA cycle (No. 6) with 34.0% and 7th place ranked No. 7 guidelines and other documentation tasks with 32.1%. Finally, the No. 1 code without management attention with 29.5% is worth mentioning.

These values allow the following **hypotheses**:

- The organisations have underestimated the tasks involved in building and establishing the ISMS,
- Lack of implementation experience in a security project,
- Lack of support or project expertise,
- Lack of management attention to the topic,
- Process models that are not aligned with local government, lack best practices, lack appropriate tools, etc.

Against the background of these results, the development of a process model specific to local governments was pursued to contribute to the elimination of the identified deficits. The analysis of existing process models or approaches for introducing an ISMS in the public sector has shown that they are either insufficiently adapted to the needs of the public sector or that they could, in principle, be adapted to the needs but are therefore, not manageable for the municipalities. In principle, it is conceivable, e.g., to use the industry standard TOGAF (see Chapter 4) with its extensions for IT security management. However, research has made it clear that small organizations are overwhelmed by the complexity of TOGAF in capacity or find it impractical, even if the general approach to TOGAF is considered sensible (Alm and Wißotzki, 2013).

7.4 Development with TOE and TOGAF

According to *TORNATZKY* and *FLEISCHER,* the TOE framework provides the theoretical foundation for the research (Tornatzky et al., 1990). The framework represents the adoption and implementation process of technological innovations in a frame of reference. The problem of the carried out study was transferred to this basic structure, and the model was interpreted to meet the specific requirements of the domain of local government. The results obtained based on the codes were assigned to the three dimensions (organization, technology, and environment) of the TOE framework. At the same time, the TOE model was supplemented by other objects of observation since, according to *DiMaggio/Powell*, organizations are influenced by three specific mechanisms: (DiMaggio and Powell, 1983) mimetic, normative, and coercive pressure.

Mimetic Pressure (Imitation pressure) refers to the behaviour of competing organizations and results from the perceived success that another organization supposedly achieves through adoption. Accordingly, mimetic pressure leads organizations to align themselves with the model of successful industry representatives structurally. There is a tendency for organizations to imitate successful organizations when there is a high degree of uncertainty due to their environment, immature or controllable technologies, or unclear objectives of their organization.

Normative pressure arises from the collective expectations of the environment. Organizations thus behave in a compliant manner to meet expectations and hence achieve legitimacy. Specifically, the widespread use of innovation (in this case, the establishment of an ISMS) within an industry means that other organisations in the same sector tend to classify adoption as legitimate behaviour. Normative pressure often arises from networking beyond organizational boundaries, e.g. with suppliers, customers and competitors.

Coercive pressure refers to formal or informal pressure that occurs due to political influences and regulations. *Formal* pressure manifests through government requirements on organizations, such as laws (e.g. EU GDPR, OZG, etc.). *Informal* pressure can arise from dependence on other organisations, such as critical suppliers or customers. They can demand compliant behaviour due to the positions of power in which they find themselves due to the centralized distribution of resources. Figure 50 below summarizes the results while highlighting the need to consider the three dimensions of the TOE framework and the specific mechanisms (pressures) in each domain when developing a solution architecture.

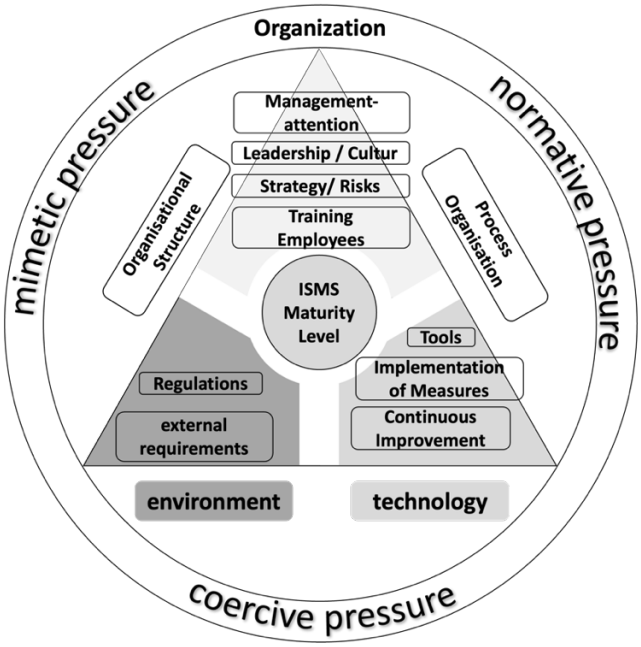

Figure 50: TOE-Framework and DiMaggio/Powell-Mechanism

Based on **TOGAF (**The Open Group Architecture Framework), a general approach for designing, planning, implementing and maintaining organizational architectures (EAM),

the[6] following process model was developed in an iterative development process. The process model's phases and structure reflect the four stages of the **TOGAF** model (Initiation, Creation, Implementation and Improvement). TOGAF thus provides the relevant basic features but falls short in certain areas, especially when it comes to adapting to the requirements of municipalities. The developed process model adapts the TOGAF model according to the requirements of municipalities; see below Figure 51**.**

The process model examines five levels at its core, starting with **compliance** and **business processes**. These two main layers are supported by the associated **application and** IT infrastructure layers **and ultimately lead to the organisation's general** building infrastructure layer **(perimeter).** In this way, a municipality's structural and operational structure can essentially be mapped, and the identified deficits can be eliminated. At the same time, these levels form the solution architecture for a municipal ISMS. Organizations that use the process model are supported along a predefined sequence of 12 steps in developing and establishing a management system.

7.5 Process model

The following process model is described from initiation to revision and transition to the first PDCA cycle: No ISMS without appropriate **management attention**! On the one hand, the first step of the process model is intended to support the creation of the necessary framework conditions at the level of the C-level, but on the other hand, to underpin the ISMS to be established using **a guideline** (policy) and to develop a corresponding hierarchy of goals, taking into account the requirements and expectations of the stakeholders (interest groups). Both the analysis of the audit reports and the literature analysis show that the consideration of **employees and their awareness** of the dangers of cyberspace are a crucial success factor for the sustainable development of an ISMS. Against this background – in contrast to many other projects or traditional standards – the integration of employees into the ISMS process is placed at the process model's beginning (2nd step).

[6] TOGAF®9.1, https://pubs.opengroup.org/architecture/togaf9-doc/arch/; Retrieved 13.06.2022.

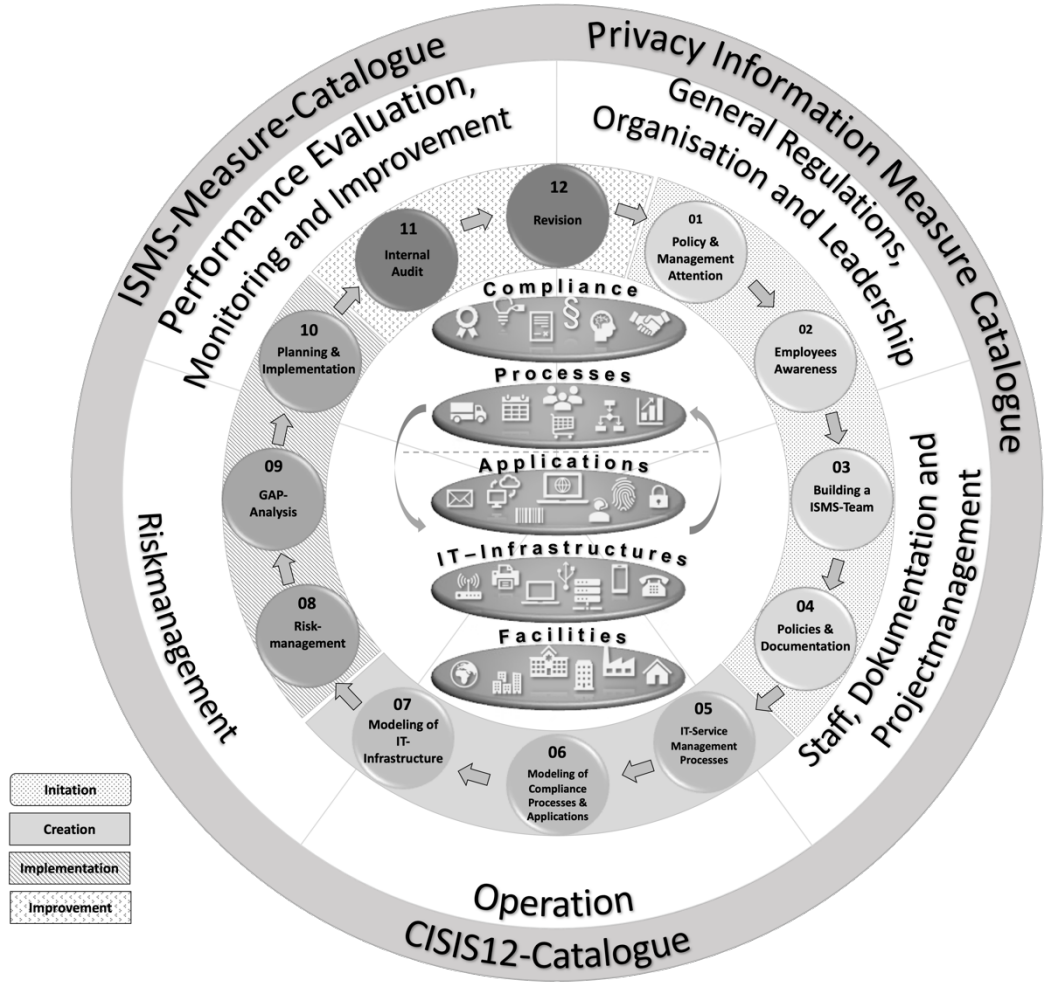

Figure 51: Overview of rough procedure model

The team composition **is essential for the successful implementation of an ISMS**. Depending on the organisation's size, it must be determined with which roles the upcoming ISMS project is to be carried out and whether further roles or expertise are to be integrated into the project. The PDCA cycle inherent in any management system puts the **P for the plan** at the forefront. No successful project without a good plan. Against this background, the next step of the process model focuses on creating and updating a documentation structure suitable for the ISMS. Documentation 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. One of the main differences from other ISMS standards is implementing **IT service management** in the process model. The implementation of clearly defined and described IT service management processes is especially a guarantee for increasing information security and the maturity level of the ISMS. The following three IT service management processes must be set up as company-specific, or the existing IT service management processes must be integrated into the ISMS and

further developed. This includes **maintenance**, **modification and fault elimination processes.** Management systems often do not sufficiently consider current **legal requirements (compliances)**. To address these compliances (especially in local government) and simultaneously lay the foundations for the expansion of the ISMS in the direction of data protection management, the **layer model** at the core of the process model in the above graphic was chosen. This also makes it easier for the organization to model measures from various organization-specific requirements or requirement catalogues. In essence, this changes the point of view. The operational consideration of organizational assets worthy of protection, such as applications, servers and building infrastructures, was brought into focus in favour of a strategic view **of compliance** and **business processes**. On the one hand, this division into a **strategic** view (management level) and **an operational** view facilitates the introduction of the ISMS (focus on core business processes) and, on the other hand, lays the foundation for strategic management of the ISMS and business processes. As part of modeling, the essential compliances and business processes are identified (taking into account mimetic and coercive pressures). Subsequently, the applications and IT infrastructures associated with the business processes are modelled and finally underpinned with appropriate technical and organizational measures from any security catalogues (e.g. from BSI Compendium, CIS Controls, ISO 27002 Measures, CISIS12 Catalogue or own security measure catalogues) to increase cyber resilience. The identified assets are subjected to a risk assessment in the next step. The current events of the last few months, in particular, have shown that developing an information security management system is no longer a hygiene factor (hygiene factor = can also be done without it, but a little worse). No, an ISMS is now a "must-have" for all organizations, and an established risk management system is an important instrument for learning from the past and being able to assess future events better and thus establish a **risk radar** for the organisation's strategic and operational perspective. Following the risk assessment, the "Assets – Processes, Applications, IT Infrastructures and Buildings" are evaluated concerning the implementation of the measures from the selected security catalogues within the framework of a group-dynamic **target-performance comparison**. As a result, a GAP analysis is available about the degree of implementation or degree of maturity of the ISMS that has already been established. The planning and implementation step follows the GAP analysis. Open measures must be prioritized by recording their financial, technical and human expenses and defining the roles of the initiator and the implementer. It is important to note that no system is perfect and that more is always possible. This also applies to the process model presented because the degree of maturity of a management system only develops with several runs (CIP process). To measure this CIP process, an internal audit is planned in the next step of the presented solution architecture. With the help of an internal audit, the organization should be able to examine its own ISMS for weaknesses and improve it accordingly. The steps presented are to be completed regularly (e.g. annually). Changes and additions can be adapted promptly, and the management system can be adapted to the dynamic challenges at any time. The final step, **revision**, summarizes the results of the

previous PDCA phase and ends with preparing a management report. This management report is supplemented by documents such as the implementation plan and risk treatment plan. It must be appropriately assessed by the management level as part of a management evaluation. As soon as the management level has approved the management report, including its assets, the next PDCA phase can begin with a new target definition, and the continuous improvement process can be initiated. The circuit supports the entire process.

7.6 Discussion and conclusions

The solution architecture presented pursues the goal of providing organizations, especially from local government, with an easy-to-implement process model with which an information security management system can be set up. At the same time, an attempt is made to define an approach to remedy the shortcomings that were revealed in the analysis of the audit reports. At its core, the hierarchical structure of the asset level (compliance to building) and the circular sequence of implementation steps facilitate the introduction of the ISMS. This cycle is supplemented on another level by higher-level elements. This addresses the strategic management of the ISMS. On the outer circular path of the architecture are the catalogues of measures to cover the mechanisms of the respective industry, as well as other requirements. With this open architecture, it is also possible to open the established ISMS to other management systems (e.g. data protection with SDM 2.0, ISO 27001, CIS controls, BSI, KRITIS §8a, etc.). During the research work, various municipalities were supported in introducing and establishing an ISMS with the help of the presented solution architecture (Moses and Sandkuhl, 2022). A positive result was achieved for all institutions. An analysis of the audit reports of the subjects from the case studies showed a significant improvement in the individual codes, and an improvement in the maturity of the ISMS and resilience could be observed. The results using the presented model are summarized in Table 24.

8 Federal Cybersecurity Architecture and Information Security Management (Post #5)

Title	**Federal Cybersecurity Architecture and Information Security Management**
Authors	Frank Moses (frank.moses@uni-rostock) Thomas Rehbohm (thomas.rehbohm@uni-rostock)
Publication Body	Moses, F., Rehbohm, T., 2023a. Federal Cybersecurity Architecture and Information Security Management - Adoption and Diffusion of the NIS-2 Requirements, in: Auth, G., Pidun, T. (Eds.), GI Edition Proceedings Band 341 6. Fachtagung Rechts- Und Verwaltungsinformatik (RVI 2023). Gesellschaft für Informatik e.V., Bonn.

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 critical 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 developing 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 speedily 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 appropriately responding 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.

Contribution to Design Science Research Step

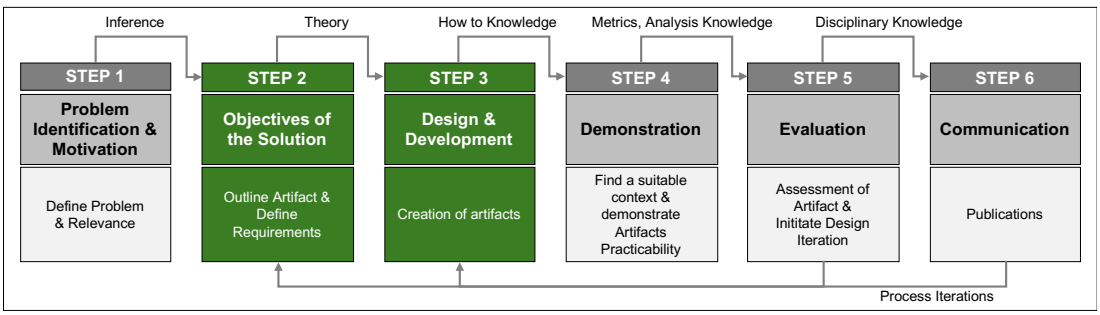

Figure 52: Publication #5 - Federal Cybersecurity Architecture and Information Security Management

8.1 Introduction (Section 1)

The availability of essential consumer goods and infrastructures is part of public services for a federal state in Germany, the respective member state and the European Union. The public administration is a guarantor at all levels of protecting the state, economy, and society (Riek et al., 2016, p. 261), (Watson and Webster, 2020, p. 261). State institutions must act since the Federal Republic of Germany and its states must place human needs, including economic ones, at the centre of their activities (Bundesverfassungsgericht, 1982).

The current threat situation leaves no room for discretion here, information security is endangered and thus higher than ever (BSI, 2022). In particular, due to successful attacks on 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.

The information security management systems of the respective actors must underpin a functionally effective and federal cybersecurity architecture. 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 should 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 (Bundesministerium des Innern und für Heimat, 2022) 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 this is 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 (Moses and Rehbohm, 2022b), (Europäisches Parlaments und Rat, 2023).

In chapter 2, we give an overview of the state of the art. This is followed by chapter “7.3 Methodology", which 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 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. The procedure model is being tested in a natural environment with different test subjects. The section 7 briefly summarises the result.

Our research aims to identify the specifics of public sector organisations and develop a Cyber Security Architecture and ISMS Approach tailored to their demands. The current requirements of the NIS-2 Directive (*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)*, 2022) should be considered.

8.2 State of the art (Section 2)

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 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, 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; instead, contributions to cybersecurity law are in current discussions (Kipker and Barudi, 2020) or civil security (Gusy et al., 2017) 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" (Rehbohm et al., 2022a). 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 collaboration architecture must emerge because, unlike governments, cybersecurity threats are borderless (Andreasson, 2012).

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 (Krajewski, 2015).

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, mainly because

trusting cooperation between the state and business is a "shared mission" (Dürig and Fischer, 2018).

8.3 Methodology (Section 3)

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) (Johannesson and Perjons, 2014). DSR is a research paradigm aiming at problem-solving in organizational settings, focusing on developing valid and reliable knowledge for designing the required solutions. DSR research projects typically consist of several phases and require different research methods depending on the DSR phase and intended design solution.

This paper concerns the design solution's phase requirements definition and design and development, i.e., the core artefact. Table 25 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 that provide information about the results.

According to the DSR paradigm, the problem must be investigated in two aspects: the knowledge base and the relevance of the business. The knowledge base generally consists 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 Cyber Security Architecture in the federal context. The business relevance has to show that the research challenge is relevant for a small number of organizations and that it is an isolated “local” problem to solve. Still, it 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 **requirements definition phase** 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 artefact 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. The artefact in its current form is documented in a handbook (already published (Moses and Sandkuhl, 2022). **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 instances. As many public sector

organisations already use the artefact, we chose a combination of real-world assessment and evaluation based on its features.

Table 25: Research activities performed in DSR phases and their results

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	Introduction (Moses et al., 2022b)
	A survey to determine business relevance	Inhibiting factors visible in the practice of Public Sector Organisations	Section 2.2 (Moses et al., 2022a)
Define Requirements	Argumentative-deductive work to derive requirements from results of problem investigation	Summary of inhibiting and success factors List of requirements	NIS 2 Directive
Design and develop Artifact	Conceptual-deductive work to design procedural model based on requirements	ISM procedural model and handbook	Summary Conclusion (Moses and Sandkuhl, 2022), (Moses and Rehbohm, 2023d)
Demonstrate	Application of Cyber Security Architecture	Not covered in this work	
Evaluate Artifact	Evaluation	Not covered in this work	

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

8.4 Federal Cyber Security Architecture (Section)

Cyber Security architectures should be an elementary component of digital services of general interest in Germany's federal system. (Schallbruch, 2018) Essential actors of a regional structure must be actively connected so that joint interaction can occur 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 53 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 (Simon et al., 2014).

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 (Rehbohm and Kalmbach, 2022), (Rehbohm et al., 2022a), (Rehbohm et al., 2022b) and (Rehbohm et al., 2021)

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, related threats to it, and associated processes.

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

Control and improvement: The steering committee assesses resilience and derives 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 processes mapped in the architecture and visualize the stakeholders' expectations.

In addition to these two dimensions of "**strategy, core and support processes" and** "**goals**", the cybersecurity architecture consists of another dimension. The users can

individually design these processes according to their respective contexts. The figure below summarizes these three dimensions (Figure 53).

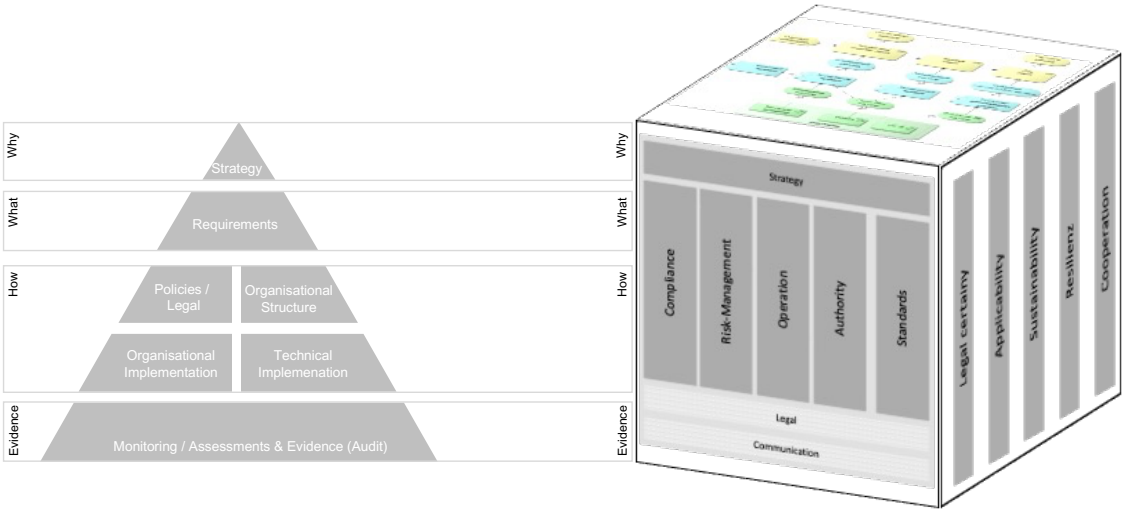

Figure 53: Cybersecurity Cube (Architecture, Goals, and Processes)

8.5 NIS 2 Directive (Section 5)

The Network and Information Systems Directive 2 (NIS-2) (Weissmann, 2023) 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: Critical infrastructure and digital service** operators 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 collaborate and share information to join the 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 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 (Eckhardt and Kotovskaia, 2023).

In Art. 21 of the NIS 2 Directive, fourteen **core requirements** are formulated that must be met by an ISMS (Weissmann, 2023). 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 implementation of the cyber security architecture. The definition of requirements for the respective context follows this. 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.

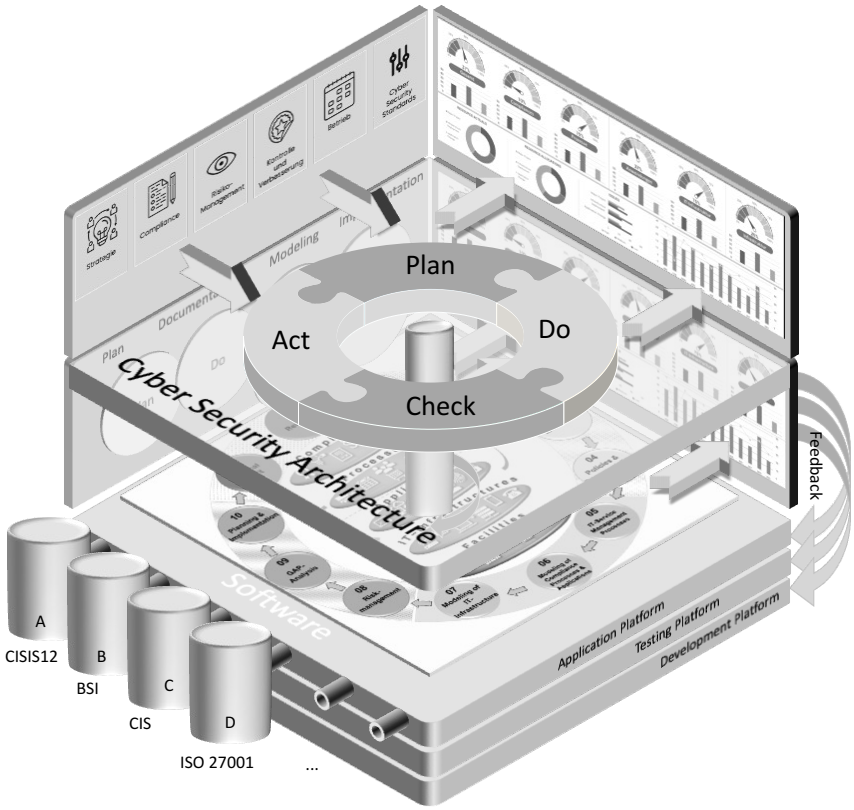

Figure 54: Cyber Security Architecture with ISMS

The elements of the cybersecurity strategy are complemented by the cybersecurity strategy (Figure 54**)**. After the theoretical derivation, strategy, requirements, and implementation measures must 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 which standard (BSI baseline protection, ISO/IEC 27001, or others) should be used to set up and establish the ISMS.

8.6 CISIS12 (Section 6)

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 (Moses et al., 2022a). Here, the CISIS12 (Compliance and Information Security in 12 Steps) process model (Moses and Rehbohm, 2023d) offers a quick and accessible introduction to the topic of ISMS for public organizations (Moses and Sandkuhl, 2022).

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 (Moses et al., 2022a), **Step 2 Raising awareness among employees**:

In many projects, the consideration of employees is only at the end of the project (Tatiara et al., 2018). 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 employee training, sensitisation, and information. 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 developing the ISMS are fixed here in writing, tasks, rights and obligations are defined, and an ISMS team is formed. Depending on the organisation's size, it is necessary to determine which roles the upcoming ISMS project is to be carried out, 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 (Choejey et al., 2016). **Step 4 IT documentation structure**: The PDCA cycle inherent 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 creating and updating a documentation structure suitable for the ISMS (Susukailo et al., 2022). Documentation 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 controlled. **Step 5 IT service management**: One of the main differences from other ISMS process models is implementing IT service management in the CISIS12 process model. Implementing clearly defined and described IT service management processes is a key success factor for increasing information security and maturity of the ISMS (Awan, 2017). 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 the management level: "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 essential business processes 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, such as 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 (Chodakowska et al., 2022). Thus, a simplification for the user also occurs here. In this way, attention can be drawn to implementing the module and measure assignment. **Step 8 Risk management**: Risk management is a major innovation in the CISIS12 process model (Kitsios et al., 2022). 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 assessing future events better. **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 a group dynamic process framework and represents a self-evaluation. External third parties may support this process. **Step 10 Implementation**: If necessary, 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. 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 include the respective certification and internal audits. With the help of internal audits, the organization should be able to examine its own ISMS for weaknesses and improve it accordingly (Pohlmann, 2019). **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 preparing a management report. Step 12 summarizes the results of the final PDCA phase and ends with preparing 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 (Preis and Susskind, 2022). The CISIS12 circuit supports the entire process – possibly tool-based.

8.7 Summary, Conclusions and Outlook (Section 7)

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 provides an open architecture. 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 53).

One limitation of the present work is that the presented theoretical cybersecurity architecture has not yet been evaluated practically. We are planning to verify the architecture in conjunction with establishing an ISMS in a municipal organization. The final logical step is to assess the overall architecture in the country's 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.

9 Requirements and Design of a Procedural Approach (Post #10)

Title	**Information Security Management in Small Public Sector Organisations: Requirements and Design of a Procedural Approach**
Authors	Frank Moses (frank.moses@uni-rostock) Kurt Sandkuhl (kurt.sandkuhl@uni-rostock)
Publication Body	Moses, F., Sandkuhl, K., 2024. Information Security Management in Small Public Sector Organizations: Requirements and Design of a Procedural Approach. Complex Systems Informatics and Modeling Quarterly (CSMIQ) 54–68. https://doi.org/10.7250/csimq.2023-37.03

Abstract

The increasing digitalization of enterprises and public authorities has resulted in the growing importance of information technology in everyday operations. In this context, an information security management system (ISMS) has become essential for most organizations. The dependency on technology for almost every single process in an organization has put ISMS at the top of the corporate agenda of public sector organizations. For public organizations, in particular, the NIS 2 Directive describes abstract requirements for developing an ISMS. On the other hand, only a few public administrations operate an ISMS. In this context, this article analyses the requirements of the NIS-2 Directive. It complements them with the obstacles and reasons for success in introducing ISMS in small public sector organizations (SPSO). At the same time, minimum requirements should be defined that help municipal administration set up an ISMS quickly and easily. This article summarizes the different requirements and generates a foundation for a rough procedural model for implementing the upcoming requirements of the NIS 2 Directive in local governments. The article also presents the conceptual design of the procedural model.

Contribution to Design Science Research Step

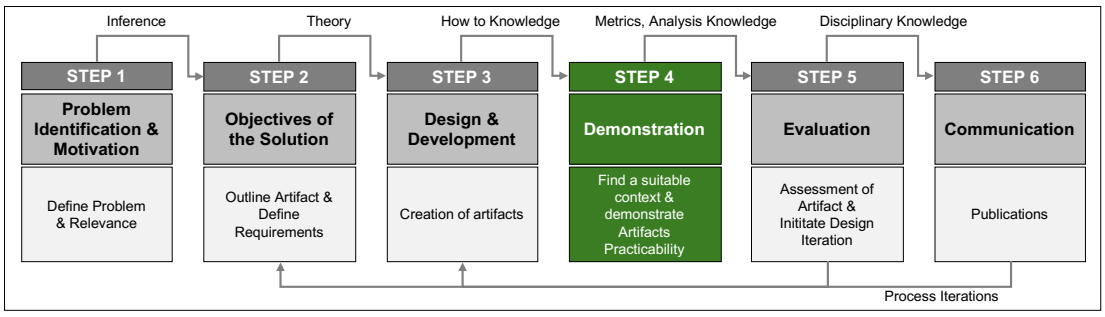

Figure 55: Publication #10 - Information Security Management in Small Public Sector Organisations: Requirements and Design of a Procedural Approach

9.1 Introduction

The dependency on technology for almost every single process in an organization has put information security management systems (ISMS) and their success factors at the top of the agenda for enterprises, public authorities and other organizations. The growing number of malicious cyber-attacks and their severity receive more and more attention in the public discussion. The information belonging to sensitive and critical organizations must be secured. Malicious cyber activities mainly include business disruption, data and property destruction, and theft of financial or sensitive data (Riek et al., 2016, p. 261). Risks and threats that can impact information security, in general, affect the confidentiality, availability, and integrity of corporate resources, causing difficulties for both large and small companies, and especially the public sector ("Raising Awareness of Cybersecurity," 2022), (Webster and Watson, 2002, p. 148).

The focus of this paper is on ISMS for the public sector. The work presented is part of an ongoing research project to develop procedural support for implementing information security management in small organization units of the public sector (SPSO). Against this backdrop, the main obstacles to implementing an ISMS in SPSOs are gathered from the literature, and a foundation for creating the first procedural model approach is derived from this.

In many centralized governmental structures, guidelines, recommendations, or even mandatory standards exist for setting up and operating an ISMS. However, in small federal governmental structures, this is often not the case (Moses et al., 2022b) which establishes the responsibility for ISMS on the individual organisation. Furthermore, these organizations are heterogeneous in size, structure, administrative tasks, duties, and resource availability. Due to this diversity, many general approaches for ISMS are not applicable. This also coincides with the author's experience after more than 25 years in a leading position in ministerial administration. Our research aims to identify the specifics of small public sector units and develop an ISMS approach tailored to their demands. The current requirements of the NIS-2 Directive (*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)*, 2022) should be considered.

Section "Methodology" describes the phases of the Design Science approach, which progresses step by step.

Section "Identifying the requirements for the adoption and diffusion of an ISMS" is divided into three subsections. First, identify the requirements that can be derived for the SPSO from the NIS-2 guideline. Second, a summary of the results of the literature review conducted. This provides an overview of the barriers, which is also the basis for further research. Thirdly, these two results are compared.

These results were structured further to develop and describe a rough process model based on them.

In the fourth section, a rough process model is derived from the requirements and described. This process model has already been successfully tested in an artificial environment. The procedure model is being tested in a natural environment with different test subjects.

9.2 Methodology

This work is part of a research project aiming at methodical and technological support for information security management in small public sector organization units. The project follows the paradigm of design science research (DSR) (Johannesson and Perjons, 2014). DSR is a research paradigm aiming at problem-solving in organizational settings, focusing on developing valid and reliable knowledge for designing the required solutions. DSR research projects typically have several phases and require different research methods depending on the DSR phase and intended design solution.

This paper concerns the design solution's phase requirements definition and design and development, i.e., the core artefact. Table 26 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 that provide information about the results.

Table 26. Research activities performed in DSR phases and their results

DSR Phase	Research activity	Result / Artefact
Problem Investigation	Literature analysis to determine the state of research A survey among small-scale Organizations	Inhibiting factors and critical success factors visible in literature and NIS2-Directive
Define Requirements	Argumentative-deductive work to derive requirements from results of problem investigation	Summary of inhibiting and success factors List of requirements of NIS-2 Directive
Design and develop Artifact	Conceptual-deductive work to design a Foundation of a procedural model based on requirements	Rough procedural model
Demonstrate	Not covered in this work	
Evaluate Artifact	Not covered in this work	

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

9.3 Problem Investigation and Relevance

Small and medium-sized local government organisations, in particular, are increasingly the target of attacks from cyberspace (BSI, 2022, p. 68). The PhD project follows the paradigm of design science research. It starts with an analysis of (a) existing scientific work in the field of information security management (ISM) for local governments and (b) an analysis of typical problems in local government's ISM as visible in information security audit reports. The detailed results of both steps are available in (Moses et al., 2022a).

The target group studied is facing more and more challenges. The complexity of information technology, the increasing degree of networking and the simultaneous dependence on IT-supported processes require that the security of information technology be given a high priority. On the other hand, legal requirements such as the EU Directive on Network and Information Security (NIS2 Directive), the General Data Protection Regulation (GDPR), the Online Access Act (OZG) and the E-Government Act continue to advance digitalisation in local government.

The increased reliance on modern ICT has significantly increased the risk of information infrastructures being compromised by deliberate attacks from within and outside, negligence, ignorance or technical failure, both qualitatively and quantitatively (Leeser, 2020, pp. 86, 107), (Pohlmann, 2018, p. 196).

Poor information security can lead to disruptions in task performance, reduce public authorities' performance, and, in extreme cases, bring their business processes to a standstill (Henseler-Unger and Hillebrand, 2018, p. 688).

In further articles by the authors, the results that could be achieved with the developed prototype of the procedural model in a field test were described. Twenty-four local governments took part in the test. As a result, it was found that a significant improvement was achieved for all of them (Moses et al., 2022b), (Moses and Sandkuhl, 2022, p. 656).

The reasons presented, as well as the studies carried out and the associated results, illustrate the relevance of research in the domain of small public sector organisations.

9.4 Identification of Requirements for the Adoption and Diffusion of ISMS

9.4.1 Requirements from NIS-2 Directive

The Network and Information Systems Directive 2 (NIS-2) 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: (Weissmann, 2023)

- **Mandatory security requirements**: Critical infrastructure and digital service operators 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 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 (Eckhardt and Kotovskaia, 2023). In Art. 21 of the NIS-2 Directive, **14 requirements** are formulated that must be met by an ISMS (Weissmann, 2023). 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 suppliers
- **Procurement**: Security in the procurement of IT and network systems
- **Effectiveness**: Requirements for measuring cyber and risk measures
- **Training**: Cyber Security Hygiene of employees
- **Cryptography**: Specifications for cryptography and, where possible, encryption
- **Staff**: 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 NIS-2 Directive provides a simple framework. First and foremost, the **organisation** must formulate a strategy. The definition of requirements of the context follows this. The organisational and **technical implementation** of the requirements must be coordinated by an appropriate **organizational structure** and flanked by proper **guidelines**. However, descriptions of the concrete implementation of an ISMS remain open (Werner et al., 2022, p. 284).

9.4.2 Requirements extracted from Literature Review

To collect the relevant literature on the status quo of information security in the public sector and especially in local government, a structured literature analysis based on *WEBSTER* and *WATSON* (Watson and Webster, 2020) was carried out in the established electronic literature database SSOAR (administrative sciences), EBSCO Econ Lit and WISO (public service) as well as Scopus (various disciplines).

The literature analysis was based on a free-text search using the combination of the following terms: "cybersecurity, public sector, information security, hindering factor, obstacles". In the first step, the literature databases were searched with German and English search terms. The first search queries resulted in around 1,500 hits, whereby a search period of 15 years was chosen. This search period was then successively restricted and ultimately limited to the period from 2016. This reduced the number of hits to approx. 703 articles.

After reviewing the titles, 378 of the abstracts were read. This was followed by a full review of the text of 165 articles. After assessing their relevance based on content, quality, and citation frequency, **92 articles** were filtered out, which were included in further analysis. The results of the search queries can be summarized as follows (Table 27):

Table 27: Result of the literature review

search string join with AND	literature-database	hits	relevance
isms, success, factor	Scopus	269	26
isms, success-factor		172	17
isms, hindering, factor		16	4
cybersecurity, hindering, factor		6	1
cyber, security, hindering, factor		10	2
cybersecurity, municipal		20	8
information, security, municipal		412	23
information, security, success factors, isms		21	9
isms, success, factor	EBSCO EconLit	8	0
isms, success-factor		4	0
isms, hindering, factor		0	
cybersecurity		151	5
information, municipal		1	1
information, security, municipal		20	1
information, security, management, system		28	0
cybersecurity	SSOAR	37	2
security, municipal	WISO	137	1
isms		4	1
information security		24	1

Table 28 presents the results of a literature review. The publications identified with this analysis were examined for factors inhibiting or supporting ISMS implementation. Sixty inhibiting factors or critical success factors were identified from the literature review.

Behind each hindering or success factor, the reference is listed in brackets [*citation*] (Table 28). On the one hand, this summary serves as the basis of this paper in the sense of Design Science Research (DSR), which is an overview of the disruptive factors of an ISMS. But also as a foundation for further research work. The determined requirements that are important for this paper (dissertation) are marked in **bold** in Table 28.

Table 28: Identified Hindering Factors resp. Critical Success Factors

Factor / Requirement	Factor / Requirement
1. Change management (Choejey et al., 2016)	2. Incentives (Tariff Structure) (Glaspie and Karwowski, 2018)
3. Application Security (Çubuk et al., 2022)	4. Cybersecurity Architecture (Rehbohm et al., 2022b), (Taddeo, 2019), (Nather, 2018)
5. Audits (Choejey et al., 2016; Glaspie and Karwowski, 2018; Khansa et al., 2017), (Susukailo et al., 2022)	6. ISMS-Organization (Choejey et al., 2016), (Poehlmann et al., 2021)
7. **Risk Management** (Preis and Susskind, 2022), (Gedris et al., 2021; Kitsios et al., 2022; Moses et al., 2022a; Susukailo et al., 2022), (Poehlmann et al., 2021), (Nather, 2018)	8. **Education Level of Employees** (Glaspie and Karwowski, 2018), (Nikolova, 2017), (van Steen and Deeleman, 2021), (Gedris et al., 2021), (Koza, 2021)
9. **Awareness of Employees** (Choejey et al., 2016), (Glaspie and Karwowski, 2018), (Chodakowska et al., 2022), (Benson et al., 2019), (Arbanas and Žajdela Hrustek, 2019)	10. Size of the Agency (Forrester et al., 2022)
11. Disaster Recovery Planning (Çubuk et al., 2022)	12. Document Revision (Susukailo et al., 2022)
13. Self-Interest (Moses et al., 2022a)	14. Achieved Level of Protection (Awan, 2017)
15. Control Centre (SPoC) (Rehbohm et al., 2022b), (Sabtu and Mohamad, 2021)	16. Misjudgement of the Management Level (Preis and Susskind, 2022)
17. Lack of qualified Employees (Preis and Susskind, 2022), (Chodakowska et al., 2022)	18. **Definition of Roles / Responsibilities and Communication** (Tatiara et al., 2018), (Choejey et al., 2016), (Gedris et al., 2021)
19. **Definition of Measures and their implementation** (Tatiara et al., 2018)	20. Sanctions (Glaspie and Karwowski, 2018; Khansa et al., 2017) (Chodakowska et al., 2022)
21. **Financial Resources** (Choejey et al., 2016; Cooke, 2017), (Chodakowska et al., 2022; Forrester et al., 2022; Preis and Susskind, 2022), (Zheng et al., 2019)	22. **Funding** (Government) (De Abrew and Wickramarachchi, 2021), (Koza, 2021)
23. Room for manoeuvre (Khansa et al., 2017)	24. **Business Continuity** (Jalali et al., 2019)
25. Outsourcing Quota (Farrand and Carrapico, 2022)	26. **Improvement process** (Moses et al., 2022a)
27. Individual Attitude (Culture) (Benson et al., 2019; Khansa et al., 2017), (Sabtu and Mohamad, 2021)	28. Information Exchange regarding Security Vulnerabilities (Tatiara et al., 2018), (Rehbohm et al., 2022b), (Awan, 2017), (Sengupta, 2022) and Networking (Rehbohm et al., 2022b), (Sabtu and Mohamad, 2021)
29. Obtaining Information on Cyber Topics (OSINT) (Chainey and Alonso Berbotto, 2022), (Potter and Hurley, 2020), (Gedris et al., 2021)	30. Government Interest (Moses et al., 2022b)
31. **Communication** (Choejey et al., 2016)	32. Concrete Measures of Security Strategies (Awan, 2017)

Factor / Requirement	Factor / Requirement
33. Continuous Improvement (Tatiara et al., 2018), (Moses et al., 2022a)	34. Loss of control (Farrand and Carrapico, 2022), (Koza, 2021)
35. Cultural Context (Benson et al., 2019), (Sabtu and Mohamad, 2021)	36. **Leadership** (Moses et al., 2022a)
37. **Policies** (Alkhudhayr et al., 2019; Arbanas and Žajdela Hrustek, 2019; Chodakowska et al., 2022; Choejey et al., 2016; Cooke, 2017; Glaspie and Karwowski, 2018; Hui-Lin and Kuei-Min, 2014; Schmitz-Berndt and Chiara, 2022; Tatiara et al., 2018)	38. **Management attention** (Moses et al., 2022a), (Arbanas and Žajdela Hrustek, 2019)
39. **Integration of the Management into the Security Process** (Tatiara et al., 2018), (Sabtu and Mohamad, 2021)	40. Measurements (Moses et al., 2022a)
41. **Human Factors** (Benson et al., 2019; Glaspie and Karwowski, 2018; Kävrestad et al., 2021; Moses et al., 2022a; Poehlmann et al., 2021)	42. Level of the Critical Infrastructures (Awan, 2017)
43. **Emergency Planning** (Jalali et al., 2019)	44. Organizational Perspective (Jalali et al., 2019)
45. Process Management (Moses et al., 2022a)	46. Productivity Loss due to cyberloafing (Khansa et al., 2017)
47. Project Management (Hui-Lin and Kuei-Min, 2014)	48. **Qualified Employees** (Chodakowska et al., 2022; Cooke, 2017; Forrester et al., 2022; Poehlmann et al., 2021; Preis and Susskind, 2022)
49. **Legal Requirements** (Moses et al., 2022b), (Rehbohm et al., 2022b)	50. Review of the Implementation of Measures (Tatiara et al., 2018)
51. Risk Consciousness (Gedris et al., 2021), (Chodakowska et al., 2022)	52. Collaboration (Choejey et al., 2016)
53. **Training Measures** (Alkhudhayr et al., 2019; Choejey et al., 2016; Cooke, 2017; Nikolova, 2017; Schmitz-Berndt and Chiara, 2022), (van Steen and Deeleman, 2021)	54. Security Culture (Glaspie and Karwowski, 2018; Khansa et al., 2017)
55. Technical Equipment (Quality) (Alkhudhayr et al., 2019; Chodakowska et al., 2022; Çubuk et al., 2022)	56. Technical Security Controls (Glaspie and Karwowski, 2018)
57. Tools (Moses et al., 2022a), (Nikolova, 2017), (Sabtu and Mohamad, 2021)	58. Behavioural Controls (Glaspie and Karwowski, 2018)
59. Certification as Proof (Preis and Susskind, 2022)	60. Maturity Models (Clemith and Sicker, 2014)

9.4.3 Integration of Requirements from Literature and NIS-2 Directive

Various requirements for the development of an ISMS can be derived from the NIS-2 guidelines as well as from the literature. The literature research carried out provides the following overarching requirements:

- Management Attention
- Strategy Requirements
- Compliance and Legal Requirements
- Financial Requirements
- Organisational Requirements

- Effective Procedural Approach
- Personnel and Financial Resources

In addition to these overarching requirements, the requirements from the NIS-2 Directive can be combined with those from the literature research. Table 29 provides an overview of the requirements (Table 29) from the NIS-2 Directive and the literature review.

Table 29: Summary of Requirements

Requirement	NIS-2 Directive	Literature Review
Asset Management	X	
Authentication	X	
Business Continuity	X	X
Communication	X	
Cryptography	X	X
Effectiveness (Gap Analysis)	X	X
Emergency Communication	X	
Incident Management	X	X
Internal Audit		X
Physical Access Control	X	
Policies	X	X
Policies and further Documents		X
Procurement	X	X
Risk Management		X
Service Management		X
Staff	X	
Supply Chain Management	X	X
Training (Employees)	X	X

9.5 From Requirements to a Procedural Model

9.5.1 Requirements

These requirements have been summarised as follows. At the top hierarchical level, the requirements from the area of compliance must be met by an ISMS to be established. This is only possible if the organization has appropriate financial conditions. Within the framework of the organizational requirements, the prerequisites for management attention, organizational structure and guidelines must be created. The sub-items Business Continuity, Continuous Improvement and Audits are subsumed under Strategy. In the area of human requirements, training measures are essential to be implemented. The largest block of requirements follows this - the technical requirements for application security, infrastructure, and the associated implementation of measures. Risk management examines all requirements individually or comprehensively to determine dependencies between the individual requirements. Figure 56 summarises the results of Sections 9.4.1 and 9.4.1.

What are the requirements of the NIS 2 Directive on the one hand, and what are the obstacles on the other hand, and how can they be implemented quickly and easily through a rough process model in small and medium-sized municipal administrations?

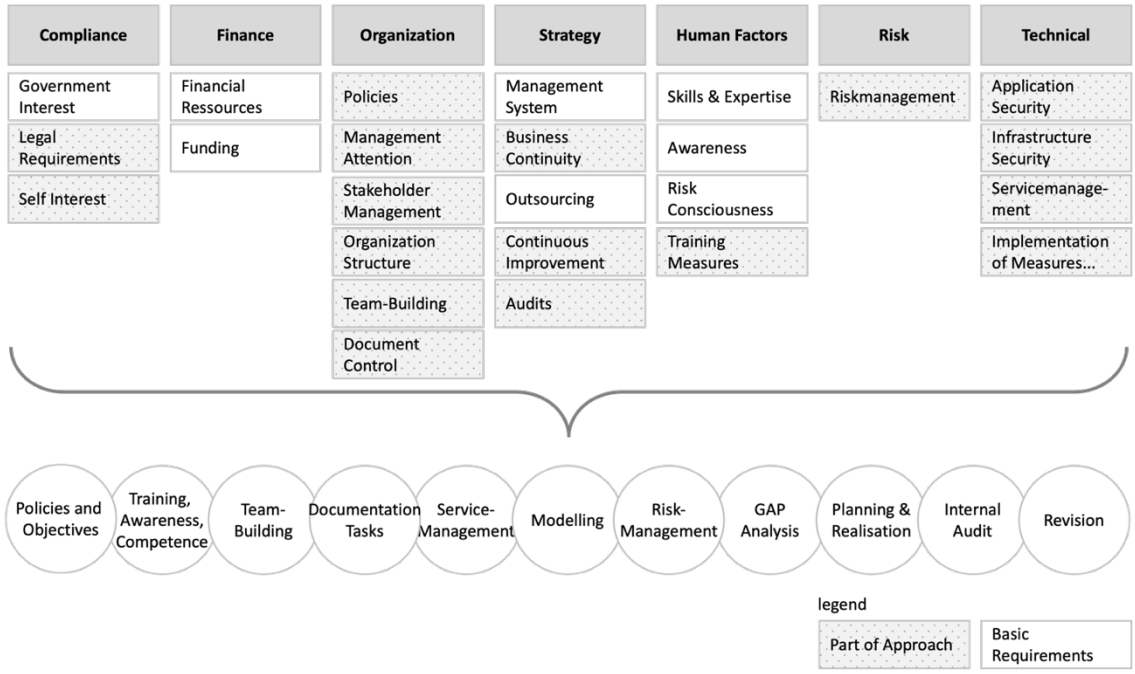

Figure 56: Structured Requirements for an ISMS as a foundation of the development of a Procedural Model

The factors highlighted in grey in Figure 56 receive specific attention in the procedural model presented in the following. The result of the literature research was that precisely these points represent a success factor for the development of an ISMS.

In a further development step, these requirements for an ISMS were transferred into a procedural model (Moses and Sandkuhl, 2022). An appropriate software prototype supports the procedural model. The procedural model and the software support (Figure 58) fulfil the requirements of an ISMS with the help of 12 steps and help to meet the requirements of the NIS-2 Guidelines.

9.5.2 Initial Procedural Model

The procedural model explains five levels, starting with the **compliance requirements** and the **business processes**. These two main layers are supported by the associated **application** and **IT infrastructure layers** and flow into the organisation's **building infrastructure layer** (perimeter) (Figure 57). The first two layers are strategic layers. The other three layers are to be understood as operational. This distinction distinguishes the presented model from different approaches, which often focus only on the operative layers (Hevner and Chatterjee, 2010, pp. 107–143).

A key point of the presented model is that compliance requirements are placed at the forefront of consideration. Concrete tasks are derived from this, especially in the area of public organizations (Hevner and Chatterjee, 2010, p. 187). However, the same applies to small and medium-sized enterprises (SMEs). In the SME sector, for example, compliance

requirements include contractual and delivery terms and conditions as andher compliances. To meet compliance requirements, processes are carried out in both types of organizations to fulfil the tasks associated with the contracts. At this interface, the process model dovetails the strategic with the operational level. Furthermore, the model ensures that both the strategic and operational areas are treated equally. Appropriate security measures will be provided for both. The implementation of these measures is supported by 12 steps in a continuous improvement process and is subject to an annual review. The latter point, in turn, fulfils legal requirements, namely Art. 32(1, d) GDPR.

Organizations that use the procedural model are supported along a given sequence of 12 steps in developing and establishing a management system.

The first step of the procedural model should, on the one hand, support the creation of the necessary conditions at the management level (C-level). On the other hand, the ISMS that is to be established should also be founded by a policy. It is also important to develop a corresponding **target hierarchy**, taking into account the requirements and expectations of the stakeholders (interest groups).

Both the material analysis of the audit reports and the literature analysis have concluded that the consideration of **employees and their sensitization** to the dangers of cyberspace are critical success factors for the sustainable development of an ISMS. Against this background – in contrast to many other projects or traditional standards – the integration of employees into the ISMS process is placed at the procedural model's beginning (2nd step).

The **team composition** is essential for the successful implementation of an ISMS. The organisation's size and the roles of the upcoming ISMS project must be determined. It is critical that a so-called core team (information security officer, IT management, data protection officer and organizational management) is established and that further roles or expertise are integrated into the upcoming project as part of an extended core team.

The PDCA cycle inherent in every management system puts the **P for a plan** in the foreground. Against this background, the next step of the procedural model focuses on creating and updating a **documentation structure** suitable for the ISMS. Documentation 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 hand, must meet the requirements of structure, clarity, completeness, comprehensibility, correctness, traceability, objectivity, integrity, and authenticity. Traceability forms one of the foundations for the ISMS's continuous improvement process (CIP).

One of the main differences from other ISMS standards is implementing **IT service management** in the procedural model. The implementation of clearly defined and described IT service management processes is a guarantee for increasing information security. At least the three essential IT service management processes must be set up organization-specifically, or the IT service management processes already existing in reality must be integrated into the ISMS:

- **Maintenance processes** (e.g. Control and execution of patch and update tasks)
- **Change processes** (e.g. On-Off-Boarding)
- **Incident Management systems often do not sufficiently consider these**

Next, the new **legal requirements**. The first level integrates these compliances into the procedural model (Figure 57). The layer model also makes it easier for the implementing organization to model measures from various organization-specific requirements or requirement catalogues. In essence, this changes the point of view. The operational consideration of organizational assets such as applications, servers and building infrastructures was brought into focus in favour of a strategic view of **compliance** and **business processes**.

This division into a strategic view (management level) and operational view facilitates the introduction of the ISMS on the one hand (focusing on the core business processes) and, on the other hand, lays the foundation for strategic control of the ISMS and the business processes.

As part of modelling, the essential compliances and business processes are identified (consideration of mimetic and coercive pressure). Subsequently, the **applications** and **IT infrastructures** associated with the business processes are modelled and finally underpinned with corresponding technical and organizational measures from any security catalogues (e.g., from BSI compendium, CIS controls, ISO 27002 measures, CISIS12 catalogue or own security measures catalogues) to increase cyber resilience.

The identified assets are subjected to a mandatory **risk assessment** in the next step of the process. The current events of recent months have shown that the development of information security management is no longer a hygiene factor (Hygiene factor = also works without but slightly worse). No, an ISMS is now a "must-have" for all organizations, and an established risk management system is a vital instrument for learning from the past and better assessing future events, thus establishing a risk radar for the organisation's strategic and operational view.

Following the risk assessment, the "assets – processes, applications, IT infrastructures and buildings" are evaluated in terms of implementing the measures from the selected security catalogues. This **target-actual** assessment should be part of a group dynamic process and represent a self-assessment. As a result, a GAP analysis regarding the degree of implementation or maturity level of the ISMS has already been established. External third parties may support this process.

The planning and implementation step follows the GAP analysis. Open measures must be prioritized by recording their financial, technical and personnel expenses and defining the roles of the initiator and the implementer. It should be noted that no system is perfect, and more always works. This also applies to the procedural model presented because the degree of maturity of a management system only develops with several runs (CIP process).

To measure this CIP process, an **internal audit** is planned in the next step of the presented solution architecture. With the help of an internal audit, the organization should be able to examine its own ISMS for weak points and improve it accordingly. If the organization lacks the appropriate expertise, this can also be done by appropriately qualified third parties. The steps presented must be completed regularly (e.g., annually). Changes and additions can be adapted promptly, and the management system can be adapted to the dynamic challenges at any time.

The final step, **Revision**, summarizes the results of the previous PDCA phase and ends with preparing a management report. This management report is supplemented by documents such as the implementation plan and risk treatment plan. It must be assessed accordingly by the management level as part of a management review. Once the management level has approved the management report, the next PDCA phase can begin with a new **target definition**. This also initiates the **continuous improvement process**. The entire process is supported by the presented cycle.

The presented first approach of a solution architecture pursues the goal of providing organizations, especially local governments, with an easy-to-implement procedural model with which an information security management system can be set up.

In essence, the hierarchical structure of the asset level (compliance to buildings) and the circular sequence of implementation steps facilitate the introduction of the ISMS. The five overarching management tasks, "General Regulations, Organization and Leadership", "Staff, Documentation and Project Management", "Operation", "Risk Management", and "Performance, Evaluation, Monitoring and Improvement", support this cycle. These management tasks are intended to ensure that the various basic requirements, such as management attention, financial resources and legal framework conditions, are considered from the outset. This addresses the control of the ISMS.

The catalogues of measures are located on the outer ring of the architecture to cover the mechanisms of local government as well as other requirements. With this open architecture, it is also possible to open the established ISMS for different management systems (e.g., data protection with SDM 3.0, ISO 27001, CIS-Controls, BSI Compendium, KRITIS §8a, etc.).

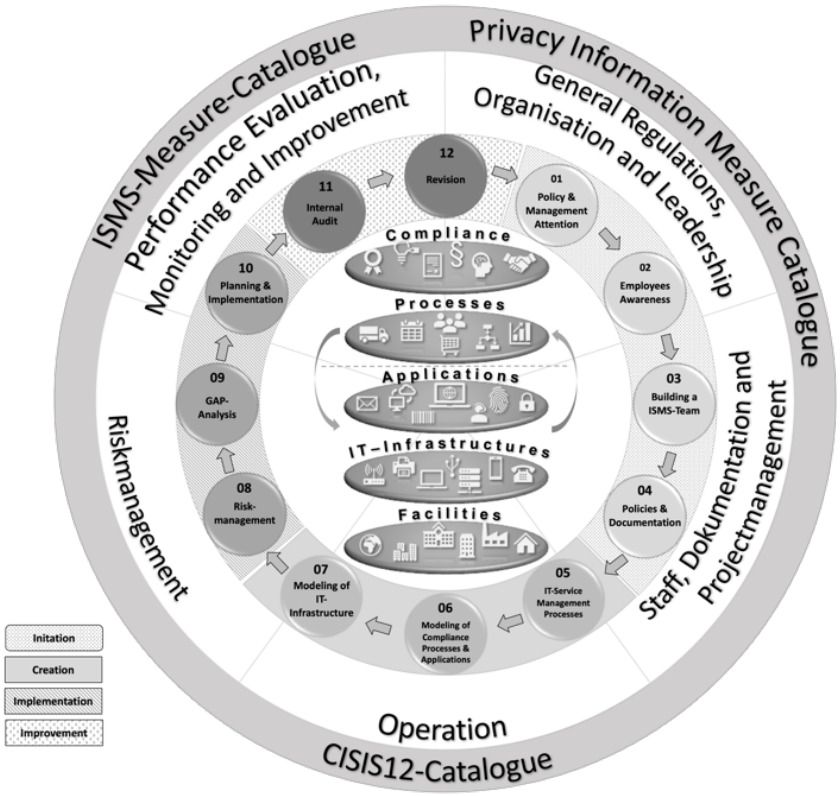

Figure 57: Initial Procedural Model

9.6 Summary, Future Work and Limitation

The requirements of the NIS-2 Directive are a very abstract framework. There is a lack of corresponding architectural concepts (Werner et al., 2022, p. 824). Below this architecture, an ISMS must be established and operated sustainably. At the same time, the requirements listed in the NIS-2 Directive meet the obstacles to the introduction of an ISMS in practice.

Through a clear identification of the requirements of the NIS-2 Directive and the obstacles described in Sections 3.1 and 3.2 and summarized in Figure 56, the foundations have been laid to create an appropriate framework for the implementation of ISMS in SPSO.

The current research project focuses on the development of such a framework. The framework conditions listed above must be considered when developing a process model. Currently, there is a first framework concept with the help of which the requirements are tested prototypically in practice. As part of the research work, the presented procedural model was integrated into a software prototype (Figure 58) and the usability was checked in an artificial environment and the field test (Moses and Sandkuhl, 2022).

Since we follow the guidelines of the Design Science Research Approach (DSR) as an overarching research design, the overall architecture (procedural model and software prototype) will be evaluated in a further step within the framework of the ongoing research

project. To this end, the specifications of *HEVNER* and *CHATTERJEE* (Hevner and Chatterjee, 2010) are to be implemented with the help of the Framework for Evaluation Design Science (FEDS) (Venable et al., 2016).

However, a limitation must be taken into account: the development of a process model specific to local governments was pursued to contribute to eliminating the identified deficits. The analysis of existing process models or approaches for introducing an ISMS in the public sector has shown that they are either insufficiently adapted to the needs of the public sector or that they could, in principle be adapted to the needs but are therefore not manageable for the municipalities. In principle, it is conceivable, e.g., to use the standard TOGAF with its extensions for IT security management. However, research has made it very clear that small organizations are overwhelmed by the complexity of TOGAF in terms of capacity or find it impractical, even if the general approach in standard TOGAF is considered sensible (Alm and Wißotzki, 2013).

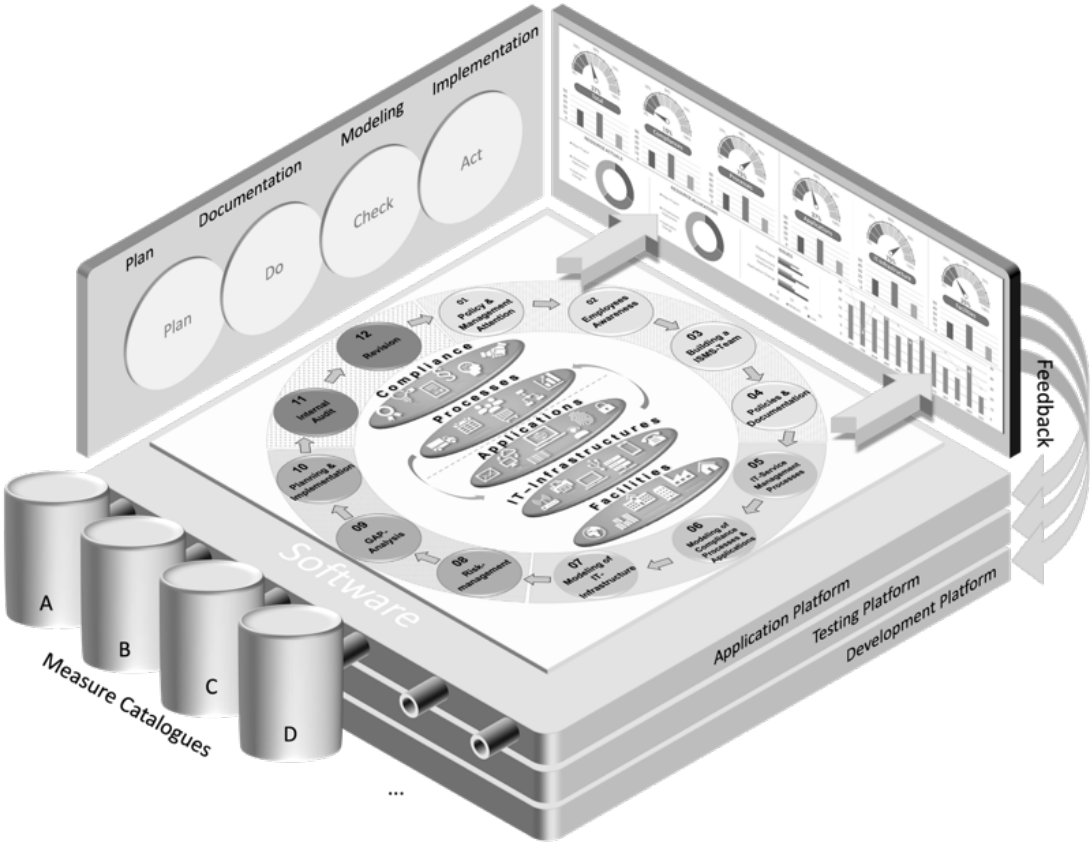

Figure 58: The Procedural Model integrated into a Software Prototype

10 Design and Evaluation of a Procedural Approach (Post #11)

Title	**Information Security in small Public Sector Organisations: Design and Evaluation of procedural Approach**
Authors	Frank Moses (frank.moses@uni-rostock) Kurt Sandkuhl (kurt.sandkuhl@uni-rostock)
Publication Body	Moses, F. and Sandkuhl, K. Information Security in small Public Sector Organisations: Design and Evaluation of procedural Approach, in Proceedings of Ninth International Congress on Information and Communication Technology, X.-S. Yan, R. S. Sherratt, N. Dey, and A. Joshi, Eds., London: Springer, 2024.

Abstract

At a time when information technology is growing faster than ever before, information security management system (ISMS) assessment has become one of the most critical aspects of most public sector organizations. In particular, the reliance on technology for almost every single process in an organization has put the issue of implementing an ISMS at the top of the agenda of public sector organizations. Public organizations must also meet requirements related to the development and operation of an ISMS. On the other hand, only a few public administrations operate an ISMS. Public organizations are hampered by many different factors, such as lack of personnel, time, money, etc., which harm the development of the ISMS. In this context, this paper briefly presents a procedural model that should help overcome the implementation hurdles in introducing ISMS in small public sector organizations (SPSOs). This process model, which has already been presented elsewhere, will be evaluated in this paper. For this purpose, an evaluation strategy is developed based on evaluation methods described in the literature, the implementation of the evaluation is described based on evaluation activities over different episodes and the results are summarized.

Contribution to Design Science Research Step

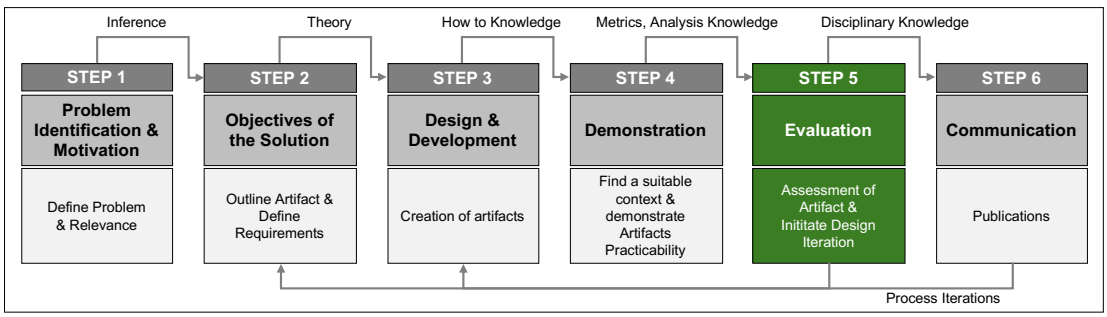

Figure 59: Publication #11 - Information Security in small Public Sector Organisations: Design and Evaluation of procedural Approach

10.1 Introduction

The reliance on technology for almost every single process in an organization has put information security management systems (ISMS) and their success factors at the top of the agenda. The growing number of malicious cyberattacks and their severity are receiving more and more attention in the public debate, and safeguards are being sought (Moses et al., 2022a). Risks and threats that can impact information security generally affect the confidentiality, availability, and integrity of organizational resources and cause difficulties for both large and small companies, especially the public sector (Moses et al., 2022a, p. 751), (Riege et al., 2009, p. 148). The presented work is part of an ongoing research project to develop procedural support for implementing Information Security Management Systems (ISMS) in small organizational units of the public sector (SPSO). Many small public organisations do not currently operate ISMS. This is due to various obstacles (Moses and Sandkuhl, 2023). In addition, these organizations are heterogeneous in size, structure, administrative tasks, responsibilities, and resource availability. Because of this diversity, many general approaches to ISMS are not applicable (Moses and Sandkuhl, 2024a). This also coincides with the author's experience after several years of project experience in ministerial administration. Our research aims to identify small public sector entities' specifics and develop an ISMS approach tailored to their needs. The approach, developed with the help of Design Science Research methods, will be briefly presented with the help of this paper, and the evaluation process will be presented. For this purpose, the evaluation methods and techniques from the literature are summarized in the first step. This is followed by a presentation of the chosen evaluation strategy before describing the previous evaluation episodes and related activities.

10.2 Procedural Approach for the establishment of an ISMS in small public sector administrations

Cybersecurity threats have changed in recent years and are steadily increasing. Even small administrative organizations are now the focus of these cyberattacks. Therefore, the need to introduce an ISMS is growing increasingly in this domain. Due to the particular requirements of small administrative units (SPSOs) in particular, the researchers have developed the procedural process model CISIS12[7] (Moses and Sandkuhl, 2022), (Moses and Rehbohm, 2023b) and (Moses and Sandkuhl, 2024a, p. 61) a part of an overall architecture (Figure 60), which attempts to minimize or eliminate the existing hurdles to the introduction and establishment of an ISMS (Moses and Sandkuhl, 2023).

[7] CISIS12 – Compliance, Information Security in 12 Steps

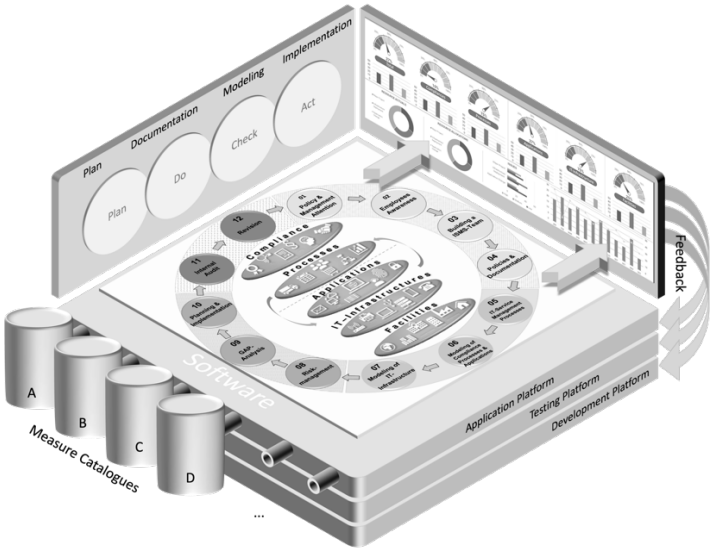

Figure 60: Procedural process model (CISIS12) incl. integrated software support

Along a higher-level PDCA cycle, the introduction and establishment of an ISMS are supported by twelve steps that must be completed in a cycle. This includes creating a guideline, training employees, building a project team, and creating a set of policies and instructions (steps 1 to 4). At the core of the model, the essential assets of the organization are focused. Security measures from any catalogue of measures can be assigned to the assets for safeguarding. In addition, the level of security that has already been achieved is evaluated, and measures need to be planned for further implementation (steps 5 to 11). Finally, an overall overview of the resilience of the ISMS is generated as a basis for the continuous improvement process. The procedure can be carried out manually (involving much effort) or by the software developed and provided in parallel.

10.3 Methodology - Fundamentals and Evaluation Methods

The relevant literature in business informatics regards evaluation as evaluating the tangible and intangible objects used or used in a specific context (Riege et al., 2009, p. 70ff). These objects are also known as artefacts. *PFEFFERS* recommends that the researcher observe and measure how well the artefact supports a solution to the problem (Peffers et al., 2007, p. 56). Hevner further refined this approach and supplemented by the evaluation criterion of quality or goodness (Hevner et al., 2004). *HEVNER* defines evaluation as the rigorous proof of an artefact's quality, usefulness, and efficacy. However, qualitative evaluation methods must be used here (Hevner et al., 2004). A glance at the relevant literature provides a collection of evaluation methods by *SIAU* (Siau and Rossi, 1998), *HEVNER* (Hevner et al., 2004) and *PRIES-HEJA* (Pries-Heje et al., 2007). These authors cite case studies, field studies, laboratory and field experiments, surveys, simulations, action research, feature- and model-based comparisons, as well as the creation of prototypes and their prototypical use as useful evaluation methods. With the help of these evaluation methods, evaluation criteria are then applied to the respective artefacts. It is important that the selected

evaluation criteria are appropriate for the case at hand and that this is justified and documented accordingly (Riege et al., 2009). Despite the many evaluation methods, the researcher receives little support in implementing the evaluation, i.e. in the how and why (Venable et al., 2016, p. 80). This means there are no recommendations regarding which evaluation method with which criteria best suits which artefacts (Fischer, 2010, p. 101). Against this background, it becomes clear that there is not just "one" evaluation method for a problem area. Rather, according to Venable et al., the solution lies in using several evaluation methods (best-of-breed approach) to compensate for the existing deficits. At the same time, it is made clear that evaluation criteria, measures or measurement criteria depend on the evaluated artefact and the objective (Venable et al., 2012, p. 430). Therefore, Venable et al. propose using an evaluation strategy with evaluation episodes. According to the above definitions, the goal of evaluation is to evaluate or prove an artefact's usefulness, quality, and effectiveness in terms of an intended solution to the problem. Further goals and, thus, a further understanding of evaluation is shown by *HEVNER* et al.: "The evaluation of the artefact provides feedback information and a better understanding of the problem to improve both the quality of the product and the design process. This build-and-evaluate loop is typically repeated several times before the final design artefact is generated" (Hevner et al., 2004). In addition to assessing the usefulness of the problem or the quality of the artefact by using a more comprehensive catalogue of evaluation criteria, other goals can be identified, namely the degree of improvement compared to existing, alternative artefacts, identification of long-distance and side effects or synergies, etc. (Venable et al., 2016). *SONNENBERG* expands the list of possible evaluation criteria as follows: safety, efficiency, correctness, reliability, applicability, flexibility, comprehensibility, and reusability (Sonnenberg and vom Brocke, 2012, p. 391). The Individual Evaluation Methods (Riege et al., 2009), (Sonnenberg and vom Brocke, 2012), (Cleven et al., 2009) already provide a good frame of reference for developing an evaluation strategy. *FISCHER* provides a good overview of the conditions of use and application and describes various prerequisites for research methods, including evaluation situations in which research methods are suitable. *VENEABLE* et al. shed light on the timing of the evaluation (Venable et al., 2012, p. 429), (Venable et al., 2016, p. 79) and distinguish between an ex-ante, i.e. evaluation before the development of the artefact, and an ex-post (i.e. an evaluation after the development of the artefact). Furthermore, the authors extend this evaluation dimension to include the dimension of the environment, namely into a naturalistic, i.e. in the real world, and into an artificial, e.g. a laboratory environment. Another dimension is the evaluation of the result, which is divided into a formative and summative component. The formative evaluation is intended to promote the results of an ongoing development process, making it possible to actively influence the artefact. The summative evaluation evaluates whether the outcome of the process achieves the previously defined goals. Another approach is described by *FETTKE* et al. In their frame of reference for the evaluation of reference models, the authors present the dimension of research method with the directions empirical vs. analytical and the dimension derivation of the quality criteria with the directions ad hoc vs. theory-driven.

Riege et al.'s evaluation approach considers two further dimensions (Riege et al., 2009, p. 81) for evaluation. In the first case, the artefact is evaluated against the research gap. Therefore, the correct design is to be examined against the background of the defined requirements. In the second case, the evaluation takes place in the real world, i.e., it is checked whether the expected benefit exists. Thus, two evaluation models shed light on the target or deployment environment. *Helfert* et al. present further dimensions of consideration in their Design Evaluation Framework (Helfert et al., 2012, p. 56). They distinguish between pragmatic, semantic, and syntactic criteria. This approach was not pursued further in the present work, as there was no direct communication in the context of the evaluation activities. The authors *Sonnenberg* et al. extend the approaches presented above to include four evaluation activities or steps (EVAL1 to EVAL4) (Sonnenberg and vom Brocke, 2012, p. 393). In the first step, the research gap will be evaluated. In the second step, the design decision is within the development process. This is followed by the evaluation of the artefact in an artificial environment. The evaluation of the use in a natural environment is the last step of the evaluation method. Through this evaluation method, the following results are achieved step by step: Determination of the research gap and design of the artefact with subsequent proof of the applicability and usefulness of the artefact. As a result, compared to the evaluation method of *Pfeffers* (... observe and measure how well the artefact is a solution to the problem described...), which relies on feedback processes through which four evaluation activities establish an evolutionary and iterative approach (Sonnenberg and vom Brocke, 2012, p. 392). In addition, the authors assign further elements, such as input and output, as well as concrete evaluation methods and criteria for the four evaluation activities. The authors *Rosemann* et al. add an essential aspect for an evaluation. In addition to an examination of importance and accessibility, they consider an examination of applicability to be useful, especially in the case of design-oriented research (Rosemann and Vessey, 2008, p. 1). The table below summarizes the methods used by each author (Table 1).

Table 30: Dimension and evaluation methods (sorted by appearance in the text)

Dimension	Method or Activity		Literature
temporal	ex-ante	ex-post	(Venable et al.,
Environment Setting	artificial	naturalistic	(Venable et al.,
functional	formative	summative	(Venable et al.,
Research Method	analytical	empirical	(Fettke and Loos,
Quality	ad hoc	Theory driven	(Fettke and Loos,
Evaluation Approach	Research Gap	Real World	(Riege et al., 2009)
Communication (semiotics)	syntactic, semantic, or pragmatic		(Helfert et al., 2012)
Relevance	Importance, Accessibility, Applicability		(Rosemann and
Evolutionary Steps	Test in artificial / natural environments		(Sonnenberg and vom Brocke, 2012)

10.4 FEDS-Framework and Derivation of an Evaluation Strategy

In Chapter 3, various evaluation strategies were presented. The most comprehensive proposal for developing a concrete evaluation strategy for a Design Science Research project is provided by *VENEABLE* et al. (Venable et al., 2016, p. 77) with the Framework for Evaluation in Design Science Research (FEDS).

Alternative approaches are listed within an overarching implementation process along four steps (Figure 61). Furthermore, the authors point out that an evaluation using a design science research (DSR) approach does not have to be singular, i.e., it only focuses on one type of evaluation episode. On the contrary, they suggest that more than one evaluation episode should be conducted.

It is also possible to mix artificial and naturalistic evaluations as well as non-empirical, positivistic, interpretive and critical evaluation methods. This supports a pluralistic view of science because each view has different strengths, which ultimately leads to a robust or more valid evaluation (Venable et al., 2016, p. 87).

The figure (Figure 61) summarizes the four steps of the FEDS framework and the possible implementation alternatives and then explains them.

The **first step** (Explicate the goal of the evaluation) summarizes the objectives of the entire evaluation. The following different objectives can be pursued (Venable et al., 2016, p. 82):

- **Rigour**: This refers to both efficiency (the artefact causes an observed or measured result) and effectiveness (the artefact also works in the natural environment).
- **Uncertainty and risk reduction**: This objective is essential when planning uncertainties are significant and is therefore an important method for reducing risks due to planning uncertainties.
- **Ethics**: Considers the risks associated with surveys due to communication or interpretation issues.
- **Efficiency**: Here, the overarching goals are weighed against evaluating the available resources (time and money) in the implementation of the respective evaluation method (e.g., naturalistic vs. artificial).

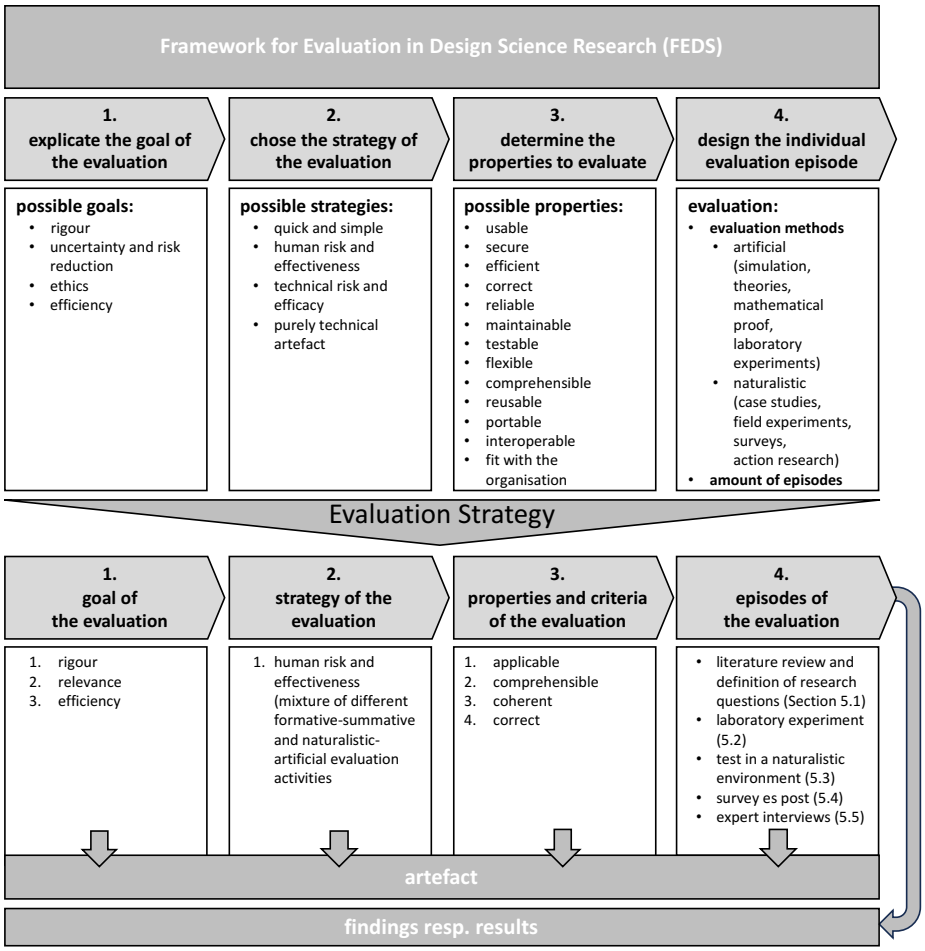

Figure 61: FEDS-Framework and Derivation of an Evaluation Strategy (own illustration)

Step 2 (Choose the evaluation strategy) selects a strategy based on the defined goals. *VENEABLE* et al. offer four alternative strategies (Venable et al., 2016, p. 82). The **first strategy, "Quick & Simple",** selects simple artefacts with low technical and social risks. On the other hand, the **fourth strategy, "Purely Technical Artefact",** is proposed only for purely technical artefacts. The other two strategies will be examined in more detail below, as they are relevant to the evaluation strategy to be developed by the researchers:

- **Human Risk & Effectiveness**: This strategy is suitable for artefacts that can be evaluated with little effort with real users in a real-world context and when user-facing and social risks are present. Furthermore, if the evaluation is to determine whether the hoped-for benefit will be achieved in real situations in the long term. In this evaluation strategy, several evaluation episodes are then undertaken. Furthermore, formative and summative, as well as artificial and naturalistic activities, are considered, emphasising a formative and naturalistic view. Evaluation methods for this evaluation strategy can be **naturalistic** (possibly relatively high resource expenditure) and **artificial** (possibly relatively high resource expenditure)
- **Technical Risk & Efficacy**: This strategy should be used when the most critical risk is technical and is too time-consuming to work with real users or natural systems in

a natural context. Furthermore, if one of the objectives of the evaluation is to determine whether the benefit is attributable to the artefact. With this evaluation strategy, formative, summative, and artificial and naturalistic evaluation activities can be carried out, emphasising an artificial and summative approach. Evaluation methods can be Naturalistic and Artificial.

Step 3 (Determine des properties to evaluate) defines the artefact's criteria, properties, and characteristics that will be evaluated later. The individual evaluation methods do not specify any specific criteria but refer to the further literature. For example, the ISO 9126 quality model includes six general dimensions: functionality, reliability, usability, efficiency, maintainability, and portability. For each dimension of this quality model, two to five properties can be used for the evaluation, e.g., under dimension maintenance, which includes analyzability, changeability, stability, and testability. This list of ISO 9126 also coincides with the lists (safety, efficiency, correctness, reliability, applicability, maintainability, testability, flexibility, comprehensibility, reusability) of *SONNENBERG* et al. (Venable et al., 2016) and *HELFERT* et al. (Helfert et al., 2012) and thus appears to be applicable.

Concrete evaluation activities are planned in **the fourth** and final **step** (design the individual evaluation episode). Since it has not been made clear in the presented models which experiences (heuristics) can be used to establish a relationship between objectives, strategies and criteria, the researcher must decide for himself how many evaluation episodes need to be carried out with the help of which evaluation method, weighing up restrictions and priorities. Based on the four FEDS steps, the evaluation strategy for evaluating the developed procedural process model for introducing an ISMS is derived in the following, summarized in Figure 61 and then described.

1. **Objective of the evaluation**: For the evaluation project, the researchers selected the Rigour and Efficiency objectives from the list of objectives proposed by *VENEABLE* et al. However, since the goal of relevance is also of great importance, especially for DSR projects, this goal was also integrated into the evaluation strategy. In the context of this goal, the Applicability mentioned above Check is subsumed (Table 30), which is an essential point in the context of design-oriented research. The procedural process model to be evaluated should be relevant and effective for management and must, therefore, be able to adapt to changing requirements.
2. **Evaluation strategy**: The procedural process model presented in Chapter 2 is a management system for developing and establishing an ISMS. In the broadest sense, one can thus speak of a socio-technical artefact. Against this background, the **Human Risk and Effectiveness Strategy** described above appears suitable for the planned evaluation. The researchers consider the resources required for assessment in a real-world context to be high. Nevertheless, naturalistic and summative evaluation activities must not be neglected. Therefore, the evaluation of the presented procedural process model is carried out with the help of a mix

(Venable et al., 2016, p. 87) of various formative and summative as well as artificial and naturalistic evaluation activities.

3. **Characteristics of evaluation activities**: An essential approach of the researchers is to create a practical benefit for a specific target group. Therefore, the following criteria must be examined from the catalogues mentioned above of criteria: **Completeness** (The artefact must contain all the essential elements of an ISMS in the target domain. Otherwise, the effectiveness in terms of functionality is not verifiable or measurable), **Coherence** (traceability with the relevant literature on comparable strategies must be ensured), **Accessibility** (Accessibility and comprehensibility for users in practice is essential for success) and **Applicability** (the applicability for the target audience).
4. **Procedure and evaluation episodes**: The evaluation was carried out through several evaluation activities and with the help of different evaluation methods. Since the research project has already been running for a long time, an immense treasure trove of data can be drawn on, and various evaluation episodes can be carried out.

10.5 Status Quo of Evaluation

Based on the evaluation strategy presented in Chapter 10.4, various evaluation episodes were carried out and described in the following subchapters.

10.5.1 Literature Review, Problem Description and Research Question

With the help of an exploratory literature search (Moses et al., 2022a), (Moses et al., 2022b) and (Moses and Rehbohm, 2023b) the research gap was examined against the real world. The identification of the problem, as well as the identification of the research gap, was carried out by an ex-ante (Venable et al., 2012) and formed the first evaluation activity (EVAL-1) of *SONNEBERG* et al. (Sonnenberg and vom Brocke, 2012). At the same time, this evaluation activity justifies the research project, including its importance and relevance. It is a formative evaluation activity, with a concretely formulated problem and research question derived from it. This research question guides the DSR process for the development of the artefact and pursues the goal of optimizing the development process.

10.5.2 Development and Laboratory Experiment

Based on the findings of the literature review and as a first approach, the procedural process model briefly presented in Chapter 2 was CISIS12 developed. In addition, a software prototype was designed to make it easy to apply the process model in practice. In this iterative development process, goals and requirements were defined (Moses and Sandkuhl, 2023), (Moses and Rehbohm, 2023b) and (Moses and Sandkuhl, 2024a). With the help of this external and formative evaluation, the development process was primarily

coordinated and adapted accordingly through several iterations. The development procedure corresponds to the evaluation activities EVAL 1 and EVAL 2 proposed by *SONNENBERG* et al. (Sonnenberg and vom Brocke, 2012). The problem or the relevance of the problem was thus identified, and the reason for the research was presented. At the same time, the first simulation of the artefact was undertaken in an artificial environment (EVAL 3).

10.5.3 Test in a natural environment

The usefulness of the presented procedural model for constructing and establishing an ISMS will be demonstrated in a natural environment. To ensure that this process can also provide prompt feedback for further development, the development group decided to develop the software prototype as a cloud solution and make it available to the test persons. This also ensures that "human" risks, according to *VENEABLE* et al. (Venable et al., 2016) are considered. The research project was started in 2018. The prototype of the procedural process model and the software were available in the summer of 2019. This was reflected in the evaluation activity EVAL 3 by *SONNENBERG* et al. As a first step, several organizations in the target domain have agreed to actively participate in the research project (Moses et al., 2022b). As part of these subjects' active supervision, the procedural procedure model and the supporting software were further developed. During the project, these Users set up an ISMS and were audited. Across the board, a significant improvement in results was observed (Moses et al., 2022a, p. 656). Thus, the following results can be recorded:

- **Proof of Applicability (**both in laboratory experiments and in several natural environments),
- **Proof of Usefulness** (In several natural environments),
- **Proof of Comprehensively (**In several natural environments) and
- **Proof of Correctness** (Proven by successful certification).

The results were taken into account in further developing the process model and the supporting software.

10.5.4 Survey ex-post

As part of the further research work, the test group was expanded to 162 subjects over the research years 2020 to mid-2022. These test clients were interviewed in a structured interview between January and August 2022 (Bortz and Döring, 2006, p. 235ff). These are mainly users from small and medium-sized local governments and some small enterprises (comparison group), from which 333 users were interviewed directly or indirectly using a questionnaire. In addition to the evaluation of the size of the organization and the time (usage since), various criteria were examined, which are summarized in the table below. This was the fourth evaluation activity described by Sonnenberg et al. At the same time, further evaluation criteria were examined. First and foremost, **Applicability**. In addition, the

study proved that the artefact has a **universal validity**. It could also be shown that the artefact fulfils the criteria of comprehensibility and accessibility. The study showed that, in particular, obstacles and obstacles to the development and sustainable establishment of an ISMS could be improved (Figure 62) with the help of the process model compared to the beginning of the study (Moses et al., 2022a)

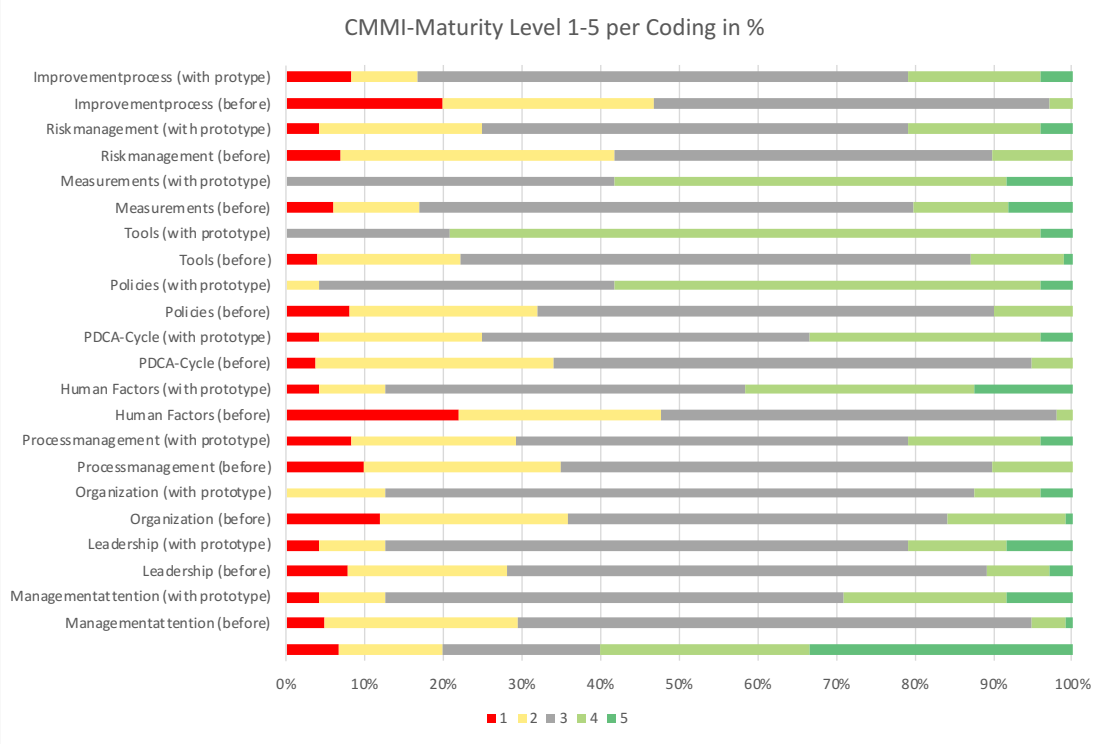

Figure 62: Evaluation of Questions

10.5.5 Further Evaluation Episodes - Expert Interviews

During further expert interviews, especially with test persons who have been working with the artefact for some time, additional findings from practice are to be integrated into the development process. The aim is to gather knowledge about whether the artefact meets the new requirements or whether adaptations are necessary to comply with environmental and technological dynamics. It should also be checked whether the artefact can be applied in other domains if required.

10.6 Summary and Conclusion

The presented procedural model for constructing and establishing any ISMS in small to medium-sized local government organizations has now undergone a development phase of several years with several iteration steps. After the normative activity to identify the research gap and the iterative development process of the procedural model and the supporting software, it was shown along the evaluation strategy that the artefact fulfils the content priorities and thus supports and improves the requirements of the research domain or the implementation process. In particular, the separation of the strategic approach from

implementation measures, as well as the support with the help of software, makes it independent of environmental or technological change. This means that the artefact can be used sustainably for the target domain. However, it can also be used in other domains through appropriate adjustments. This paper describes several evaluation activities and episodes, forming an individual evaluation strategy based on the FEDS of *VENEABLE* et al. With the help of this evaluation strategy, the present artefact was evaluated. It became clear that the design-oriented evaluation is not entirely supported by methodology. Although the chosen evaluation strategy was helpful, the evaluation process was nevertheless fraught with some difficulties. On the one hand, there is a lack of methodological support: Which target criteria and combinations of methods are helpful for an evaluation, and when is a sufficient degree of evaluation activities (saturation) achieved? A self-selected mix of evaluation activities or episodes can solve these deficits.

11 CISO – the driver of an ISMS project in public administrations (Post #12)

Title	**CISO as the driver of an ISMS project in public administrations: Role, tasks, and localisation of the CISO**
Authors	Frank Moses (frank.moses@uni-rostock) Kurt Sandkuhl (kurt.sandkuhl@uni-rostock)
Publication Body	Moses, F., Sandkuhl, K. CISO as a Driver of an ISMS in Public Sector Administrations, in Human Centred Intelligent Systems. Proceedings of KES-HCIS 2024 Conference, A. Zimmermann, R. Schmidt, L. C. Jain, and R. J. Howlett, Eds., Springer, 2024.

Abstract

The Information Security Officer (CISO) is increasingly playing a key role in combating the ever-increasing threats from cyberspace. In doing so, he must cover a wide range of activities and responsibilities, such as defining and monitoring a cybersecurity strategy, creating a security-oriented organizational culture, training employees to become more security-aware and implementing security measures. This requires close cooperation with the IT management (CTO), the data protection officer (DPO) and the organizational management (CEO). In many local governments, the role of the CISO is occupied. But in contrast to the DPO, which has been established in the organizational hierarchy for a long time due to legal requirements, the CISO is often not located at the upper hierarchical level but often in the line organization or the task is performed by external third parties. This article compares the role tasks and positioning of the CISO in companies with administrations. In addition, he examines the positioning of the CISO in administrations of different sizes based on a study carried out. Based on the literature, he describes the tasks of the CISO. He provides arguments for the optimal location of the CISO in the administration hierarchy so that cybercrime can be effectively combated.

Contribution to Design Science Research Step

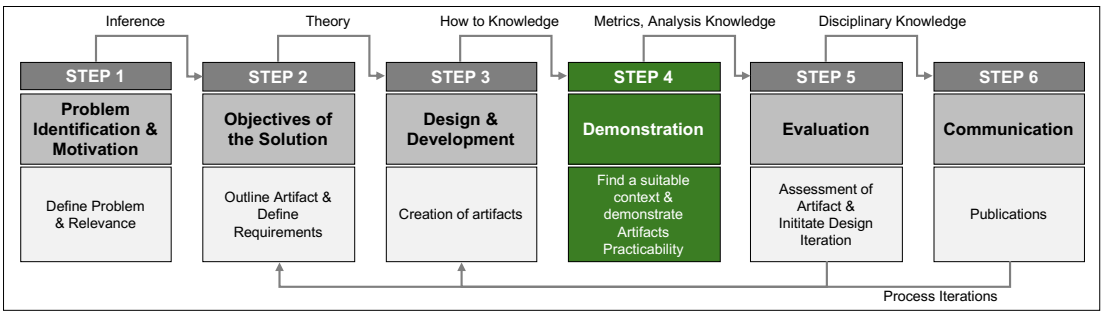

Figure 63: Publication #12 - CISO as the driver of an ISMS project in public administrations: Role, tasks, and localisation of the CISO

11.1 Introduction

The public sector is facing significant challenges to digitize itself, to consolidate an established IT landscape comprehensively and at the same time to adapt to new requirements and ensure the operation of numerous, dislocated, interconnected and often critical IT systems, taking into account the threats from cyberspace (Balta et al., 2020). The public sector increasingly needs IT personnel with the appropriate expertise to accomplish this task. This requires personnel with operational experience and management experience. These leaders must be located accordingly in the organizational hierarchy to ensure that they are heard and that their message is perceived and taken seriously by all those involved. The issue of cybercrime is a serious problem area for local governments. A vulnerability in an organization can cause the administration to fall victim to a cyberattack. The result is the outflow of personal data or the inability of the attacked administration to act. If this is the case, the person responsible is usually searched. This is quickly found, the Information Security Officer (CISO for short)! In many organizations, the CISO is located at a lower level, often directly in the IT department itself, or in small organizations, the role is performed by external third parties. Critical security projects and the increase in IT project resources are often not approved, or the CISO fights out of line. It is precisely in this circumstance that attempts are made to set up an information security management system (ISMS) from the IT department that often fails due to the decision-making powers of the CISO and is, at best, a major challenge that frustrates many CISOs in public administrations and often makes them look for other employment (Da Silva and Jensen, 2022). A local government also needs a dedicated officer to coordinate and manage the information security function (Allen, 2015). It is essential that an open communication culture is established and that the CISO can tell the truth, regardless of the personal consequences (Shayo and Lin, 2019). If this is not the case, the role of the CISO can be compared to a combination of the characters Sisyphus and Cassandra, who are known from Greek mythology. Sisyphus, punished by Hades for cheating death, had to roll a stone up a hill that rolled back to the starting position whenever it approached the target. Cassandra, who could correctly predict the future, was cursed by Apollo so that she would never be believed. Both Sisyphus's and Cassandra's suffering can be transferred to the CISO. Regardless of the type of organization, the ISB is often seen as a "killjoy" that bureaucratizes IT processes, constantly predicts disaster, and demands a higher budget.

There is, of course, a grain of truth in every statement. Still, the critical role that IT plays in today's business world – securing the information processed by IT systems – is essential to the long-term functioning of the administration (Whitten, 2008). One of the biggest mistakes that information security professionals make in local governments is that they classify (IT) security less as a business issue than a technological one(Goodyear et al., 2010; Knoll and Strahringer, 2017; Maynard et al., 2018). On the other hand, corporate cybersecurity has expanded far beyond the boundaries of IT and has become a task at the highest corporate level. The potentially devastating impact on shareholder value, market share, reputation,

and even long-term survival is now unmistakable. Cybersecurity is a topic that transcends all organizational silos and boundaries, top-down and encompasses people, culture, and risk management, bridging security, technology, privacy, and compliance (Bertschek and Janßen, n.d.; Bostelmann, 2021; Engels, 2021). This is often not the case in local governments. Against this background, on the one hand, the tasks of the CISO must be defined and anchored in the organizational structure and processes, and the role must be given a suitable function name.

11.2 The Information Security Officer in the Literature

The terms Information Security Officer (ISO) and Chief of Information Security Officer (CISO) are used differently in the literature. There is no distinction in Anglo-Saxon literature. In German literature, the two terms are often used synonymously, but also more and more often with different definitions or task approaches and, above all, a different positioning in the organizational structure (Liedtke, 2022). First and foremost, the literature discusses the increasing need for management to review, monitor and control information security in the organization under the term (IT) governance. Wong et al. consider these control tasks essential to be delegated to a particular authority (e.g. CISO) (Wong et al., 2020). The authors von *Solms* and von *Solms* suggest that information security strategies, objectives, organizational structure, risk management, and performance monitoring should be integrated into the CISO's range of tasks (Von Solms and Von Solms, 2004). The expectations placed on the role of the CISO and the responsibilities that come with this role were examined by *Hooper* and *McKissack* (Hooper and McKissack, 2016). The authors believe that not only is technical expertise necessary for the role of the CISO, but they also describe communication skills as a key competency. Communication skills, in particular, make it easier for the CISO to communicate about cybersecurity challenges with C-suite and other executives effectively. The competencies required by a CISO are examined in the study by Onibere et al. (Onibere et al., 2017). In doing so, the authors emphasize the need to conduct security campaigns to underpin the strategic importance of the CISO. In addition, they identify five key requirement characteristics: thinking, problem awareness, execution, response, and advocacy, i.e., strategic CISOs must be creative to develop effective and relevant strategies. In doing so, they must grasp the organisation's context, have a holistic view and maintain a keen awareness of the environment. They must also be able to translate visions and strategies into actionable plans and align them with organizational goals. Last but not least, they must inspire, influence, persuade, communicate clearly, negotiate and advocate for the cause. Monzelo and Nunes analyzed where the role of the CISO should be located within an organization (Monzelo and Nunes, 2019). They find that specific C-level leadership roles, such as CEO, CFO and CIO, are already established in organizations, and the role of the CISO is still evolving. They found that in the past, the CISO's role was seen more as a technical role that sets security standards and policies. At the same time, recently, it has been increasingly recognized as a

core element of the organization's cybersecurity strategy. The study also finds that in organizations where security issues are less of a focus, the role of the CISO is usually located in or even subordinated to the IT department.

On the other hand, there are organizations where the management level deals with information security risks and their impact on business operations. The CISO is independent and in excellent proximity to the management level. In the study by *MOSES* and *SANDKUHL*, the deficits of "management attention" and "lack of CISO" or "incorrect positioning of the CISO at the hierarchical level" could also be observed in particular (Moses et al., 2022a). Whether the CISO still deserves the name CISO in these cases remains to be seen. The study conducted by Karanja also sheds light on the positioning of the CISO in the organizational hierarchy (Karanja, 2017). At the heart of the study was the position of the CISO before and after a security breach. The frightening result is that out of 13 companies, six did not have a CISO before the security incident, and only 5 of these companies subsequently hired a CISO. The organizations surveyed stated that they view IT security and the role of the CISO as a technically specialized function. At the same time, the CISOs complained that they are still struggling to gain management's credibility, i.e., they are suffering from the "Sisyphean Cassandra phenomenon" already described above. IT security is, therefore, not understood as a specialized organizational function. The authors *ASHDEEN* and *SASSE* also note this and demand that IT security and the role required for it must be understood more as a strategic task(Ashenden and Sasse, 2013).

A study conducted ten years ago by *AHMAD* et al. showed that security strategies are more likely to be implemented "bottom-up" than "top-down" in organizations (Ahmad et al., 2014). The controlling safety function (ISO/CISO) was located at a middle management level or in the line function. All the study participants were unaware of a security strategy, nor was the strategy being driven by senior management. *ZWILLING'S* article confirms that this state of affairs has not changed much today (Zwilling, 2022). However, it does provide an excellent overview of the relevant literature dealing with the different tasks of the CISO (Zwilling, 2022). Finally, the author concludes that organizations need to assess their CISOs' knowledge of new cyber challenges and risks and consistently invest in improving this knowledge and new technological solutions. They should give the role an appropriate appreciation through an appropriate location in the organization. Paech and Vogel examine the necessary competence requirements of security officers by analysing job advertisements. They note that job advertisements for ISOs require a degree, but the field of study is often secondary. In addition to the skills already required by Hooper, *MCKISSACK* and *MAYNARD*, *PAECH* and *VOGEL* were able to determine that more emphasis is placed on further training in the English language as well as knowledge of the relevant standards and process models such as BSI-Grundschutz, ISO 27001, IT-Auditor, etc. (Paech and Vogel, 2022). The authors *KAPPERS* and *HARRELL* confirm this with their study from 2020 and describe a relevant degree, at least ten years of professional experience, in particular, management experience and corresponding personal certifications such as Certified

Information Security Manager (CISM) as important qualities of a security officer (Kappers and Harrell, 2020). The importance of good communication skills for the CISO is mentioned in several articles. For example, *HOOPER* and *MCKISSACK* point out that "[...] the CISO should be an excellent communicator with business knowledge and interpersonal skills" (Hooper and McKissack, 2016). The authors discuss in depth the importance of the CISO being a good communicator who can translate their technical expertise into a more appropriate language, for example, to help senior management better understand cybersecurity risks or solutions. This was also identified by *MAYNARD* et al. as one of the qualities required for a CISO: „A CISO needs the ability to negotiate, influence, and communicate clearly to become a strategist“ (Maynard et al., 2018). The (communication) ability to collaborate across organizational boundaries is also cited by Goodyear et al. (Goodyear et al., 2010) as important for the role of the CISO, as CISOs often coordinate or collaborate with IT staff in other agencies,with non-IT staff in other agencies, and with private sector (IT) service providers. In Anglo-Saxon literature, only the role of the CISO is mentioned. There is no distinction between CISO and ISO, unlike in German-language articles. A CISO is assumed to be located at the higher management level and generally has dispositive tasks. At the same time, it is assumed that the role of the CISO, like the other role holders from the C-level, has an organizational and personnel underpinning. It is precisely at this point that it becomes clear why Liedtke distinguishes between a CISO and an ISO in his definition (Liedtke, 2022). On the part of the CISO, he identifies more dispositive tasks, such as responsibilities for the entire IT security organization, as well as for IT compliance, IT risk management and emergency management. In contrast, it only assigns responsibilities in the operational area to the ISO, namely the technical safeguarding of IT and the review of the implementation and compliance with IT security requirements. This means that local governments lack the power of argumentation. Since the role of the ISO is only attributed to operational tasks, it is often not possible for local governments to establish the role of the information security officer at a correspondingly high hierarchical level. And even more, this is often not intentional. The observation of Monzelo and Nunes, already described above, namely the non-existent awareness of integrating the ISO into the management level (C-level), occurs frequently, especially in local government. A review of the organizational charts of municipal administrations shows that although many so-called representative roles are shown there, such as women's representatives, data protection officers, etc., the role of the ISB or CISO is rarely found there or, according to Meuche, have the character of a staff unit with an advisory function without any authority to issue instructions (Meuche, 2022). Taking into account the steadily increasing cybercrime, it is all the more important to establish the role of the information security officer in the right place in the administration, then to equip it with the appropriate functional name, namely CISO, and to appoint the right person for this role!

11.3 Establishment of the ISO in companies and administrations

11.3.1 Information Security Officer in Companies

In recent years, it has become established in the organizational structure of companies that function names from the American-speaking world are used, e.g. CEO (Chief Executive Officer), CFO (Chief Financial Officer), CPO (Chief Product Office) (Fitzgerald, 2007). These primary C-level designations have also been accepted in the scientific literature. In the mid-1980s, the role of the CIO (Chief Information Officer) became more and more common in companies due to the increasing importance of IT (Atanassov, 2019) and is located on the same level as the other C-level roles (Kappers and Harrell, 2020). On the other hand, the role of the CISO is still in the establishment phase in many companies (Atanassov, 2019). Companies are increasingly aware that cybersecurity risks are directly related to their innovation and growth strategies (Goodyear et al., 2010). Against this background, with the introduction of the CISO role (similar to the establishment of the CIO role), a corresponding organizational classification of the CISO role at the highest management level is to be expected or can already be observed in many companies (Auth and Von Der Heyde, 2022). The CISO is primarily responsible for strategic and communication tasks and, like the other C-level functionaries, has a corresponding budget and assigned personnel.

11.3.2 Information Security Officers in Administrations

The term CISO has only established itself in public administration at the federal and state levels (Remy and Stettner, 2021). In local governments, presumably also due to the inflationary use of the term information security officer and its definition by the Federal Office for Information Security (BSI), an inappropriate term with an outdated definition of the term has established itself in the minds of administrative managers. The definition of the role is „Information security officers are persons appointed by the head of the institution who coordinate the task of information security on behalf of the management level and promote it within the authority or the company.“ (BSI, 2023) falls short. Also, the slightly different definition in the context of the glossary of the BSI Compendium 2023 „The Information Security Officer (ISO for short or, more rarely, IS Officer) is responsible for the operational fulfilment of the "Information Security" task. Other designations include CISO (Chief Information Security Officer) or Information Security Manager (ISM), which equate the term Information Security Officer (ISO) with Chief Information Security Officer (CISO). Although the BSI still mentions the term information security manager, the confusion is even greater. This definition is an attempt to make it clear that the role of the information security officer is also an outstanding and essential task in the administration, which should be anchored accordingly in the organization. However, there is no reference to the location and concrete task descriptions. It can be stated that in public administrations, the role of the information security officer appears in the business distribution plan and more rarely in the organizational chart but is still not located at the hierarchical level corresponding to the

role, nor do the job descriptions in the business distribution plan correspond to the role (Lanz, 2017).

11.4 Positioning of the ISO/CISO in public administrations

To determine whether and at what hierarchical level the information security officer is established in a municipal, district council or city administration, the researchers conducted two studies. In the first study, 421 audit reports from local governments were analyzed and examined, particularly the organizational structure (Moses et al., 2022a). It was found that the organizations that had already set up an ISMS and had undergone an external audit had each appointed a person concerning the information security tasks. However, no conclusions could be drawn from this about the position of the information security officer in the respective organization. Therefore, in the second study, a total of 162 administrations were asked at which hierarchical level the ISO is located in the respective organization. As a result, five positions were mentioned by the administrations surveyed:

- External ISO
- ISO in the line, IT department, or subordinate to it
- ISO in line with independent reporting tasks to management
- CIO and ISO in personal union
- ISO/CISO with a clearly defined task structure as an equivalent C-level board member

In the study, the hierarchical level of the ISO was positioned in the respective organization, and the organisation's size concerning the employees was also considered (Figure 64). It is noticeable that, especially in small administrations (up to 25 employees), one ISO is named by all of them. However, this is only located in the line organization or is even supported by an external company. This ratio does not change significantly for administrations with up to 150 employees. There, 5% (n=42 of 162) of ISOs already have the right to speak directly to the management level. On the other hand, 25% (n=42) of ISOs are still represented by external third parties. Around 70% (n=42 of 162) are also located in the line organization for this organization size.

The picture changes in organizations with up to 250 employees. Only about 17% (n=12 out of 162) of administrations outsource the task of information security officer to external third parties. 75% (n=12 out of 162) of the administrations place the ISO in the line organisation, and 8% (n=12 out of 162) give the ISB the right to speak directly to the management level. In administrations with up to 500 employees (usually city administrations or district offices), a significant improvement in the positioning of the ISO can be observed. None of the administrations surveyed relies on the expertise of an external ISO. Although most ISOs are still in the line organization, 45% (n=18 of 162) already have the right to speak directly to the management level. Even one administration (5% - n=18 out of 162) has directly assigned

information security tasks to the CIO (in this case, the mayor). Large administrations with over 1,000 employees were surveyed only nine times in the study. This group relies only on internal ISOs, with ISOs with direct right of first refusal dominating at 56% (n=9 out of 162). But even here, about 22% of the ISBs are still in the line organization. In one of the administrations, the CISO is a member of the management level and coordinates information security from "the very top".

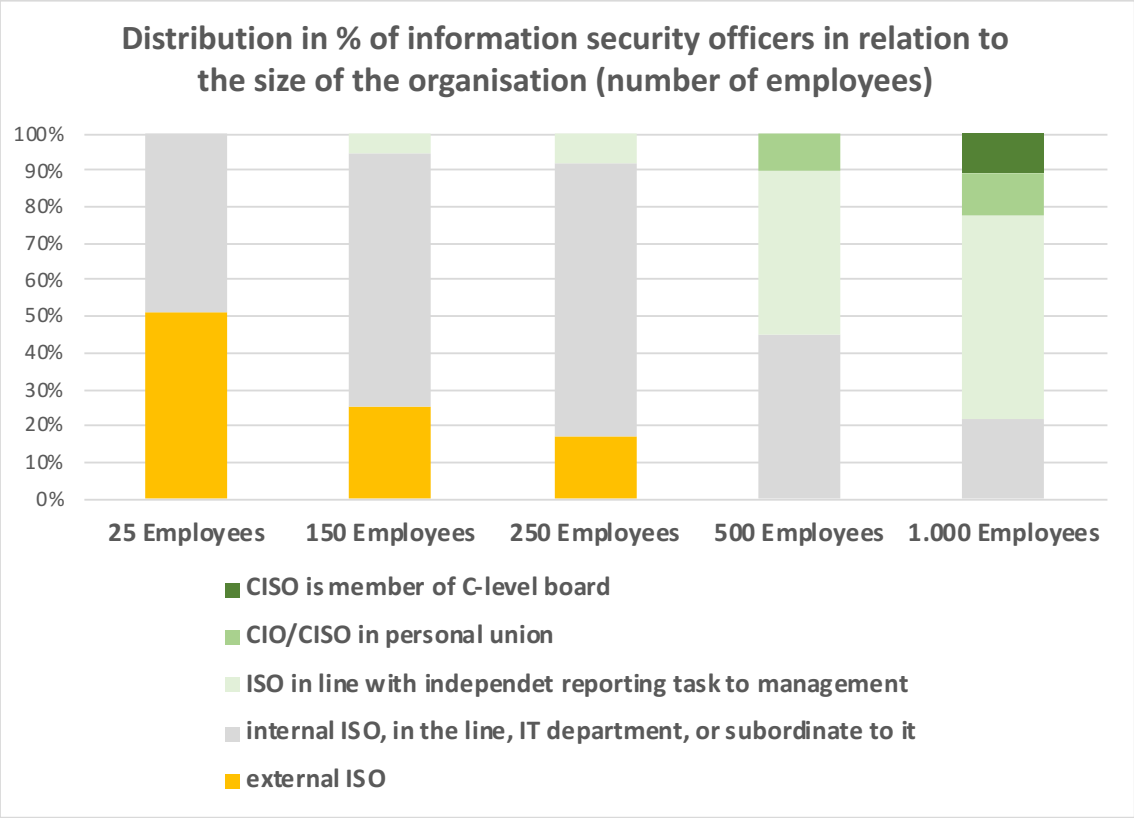

Figure 64: Information Security Officers in Administrations

Upon closer inspection, it can be seen that although ISOs are consistently named in small organizations, internal and external ISBs are balanced. As the size of the organization increases, this picture changes. The tipping point is reached at an organizational size of 250 employees. From this organizational size, the administrations have sufficient personnel substance to delegate tasks to specialized organizational units or to set up such organizational units in the first place. Large administrations such as city and district administrations often take on centralized tasks, which is why the management's attention to cybersecurity is more present here. Therefore, a corresponding delegation of functions and location of the ISO in the organizational structure takes place. At the same time, in such administrations, the tasks of the ISO are clearly defined, and the role can be found in the organizational chart at a higher hierarchical level.

11.5 Necessity, tasks and positioning of the ISO/CISO

Establishing a CISO or person responsible for information security demonstrates the need for a leader dedicated to the needs and trade-offs of information security in any organization (BAFIN, 2017). Despite the importance of the CISO's role in IT governance and the promotion of an administration's internal control structure, the organizational position and the correct designation of the CISO's role remain controversial. While regulated industries, including financial services, recognize the benefits of an independent CISO, in some sectors, most notably administration, the CISO continues to be in the IT department and usually without direct access to the C-suite (Hanschke, 2020b). Some experts believe that the CISO should report directly to the CEO (mayor or district administrator) due to the importance of this function; others believe that the CIO and CISO should be jointly responsible for protecting the organization's assets, and still others believe that organizational mapping does not matter at all. A glance at the tasks of the CISO listed in the literature quickly makes it clear that this discussion is not conducive to the necessary cyber resilience of administrations. Instead, it is crucial, as is customary in administrations, to look at the tasks and then decide to which person the range of tasks is delegated, with which personnel base, and where the person or the created organizational unit must be located within the organizational structure to achieve corresponding effects in the administration in the long term. The information security officer must perform the following tasks to ensure that all levels (Fig. 2) are served to defend against cyber risks (Lanz, 2017; Shayo and Lin, 2019):

1. Protect, shield, defend and prevent: A key task is to ensure that the administration has implemented the suitable security measures to prevent a cyberattack as much as possible.
2. Monitor, Hunt and Detect: Deploy tools that enable management to identify internal and external threats. At the same time, employees should be trained on threats from cyberspace.
3. React, Recover, and Sustain: Creating awareness that security breaches are inevitable (100% security does not exist!) and developing and implementing plans to properly manage the violation, recover compromised systems, and keep management running during the recovery process (Business Continuity Management).
4. Govern, manage, comply, train and assess risk: Active management and control of information security and the information security management system, assessment of risks and active information gathering, filtering and communication of possible risks to management and employees.

These are not just individual tasks that can be considered independently of each other and delegated to different people or organizational units. On the contrary, these tasks are components of a frame building (Figure 65) for which a role must take responsibility. The

foundation (basement) is Enterprise Architecture Management (EAM) (Hanschke, 2016) and, at the same time, is a success factor for the establishment of a sustainable ISMS or a cyber security architecture (Sowa and Rost, 2020). The entire ISMS building will be built floor by floor on this foundation. First and foremost, appropriate measures are modelled and implemented for the assets in the EAM development plan with the help of the ISMS. The ISMS is set up on the first floor, which follows the classic Deming Circle (Plan, Do, Check and Act).

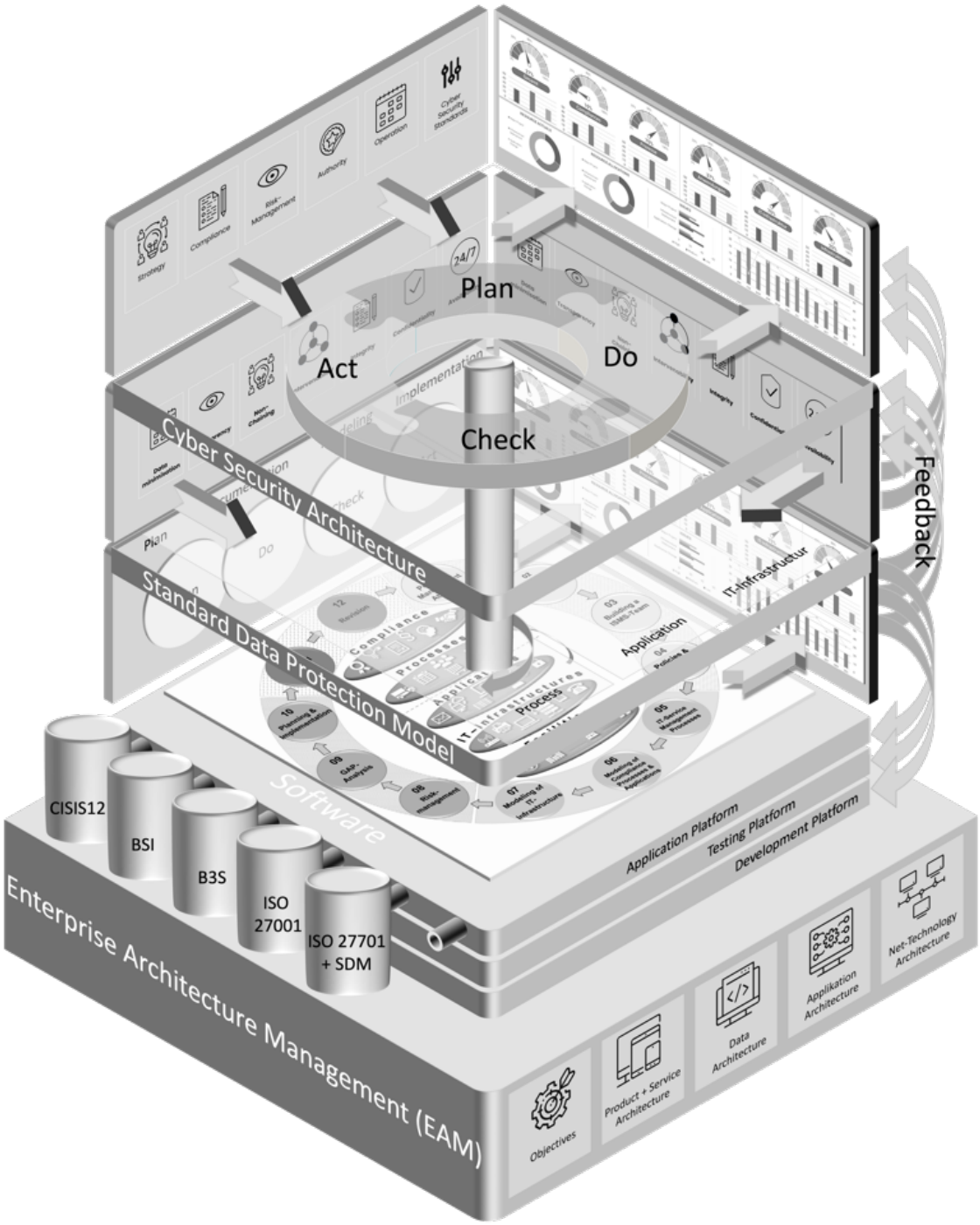

Figure 65: Architecture Building with Level EAM, ISMS, Data-Protection and overarching Cyber Security Architecture

Source: (Moses and Rehbohm, 2023b)

The ISMS will be successively established along a repetitive cycle of subtasks. With each run, the implementation of measures increases, e.g. from CISIS12, BSI or other module catalogues. The results are then available to both the information security officer and the management level, i.e. a dashboard is gradually created as an essential information, communication and decision-making tool. The second floor of the frame building is used to meet data protection requirements.

For the essential business processes of the organization, the associated specialist applications and IT infrastructures, measures and, under certain requirements, a risk assessment (data protection impact assessment) must be implemented or carried out. A tried and tested means for this is the standard data protection model (Sowa and Rost, 2020). Whether and when the tasks of the second floor are carried out is up to the management level. However, the earlier the data protection requirements are considered, the sooner the legal requirements are met, and the organization can call itself "compliant".

The main control and monitoring tasks are located on the third floor (cyber security architecture). These are tasks such as defining an overall strategy and considering compliance requirements. Other tasks include maintaining operations, considering the risks to the respective assets, and selecting the appropriate security measures for the assets from the appropriate cyber security standard (e.g. CISIS12, BSI or ISO 27001).

The overall control and definition of improvement measures is the responsibility of a joint responsibility, namely that of the information security officer and the management level, supported by a higher-level dashboard that aggregates the data from all floors below.

Communication then takes place vertically via a drive axis to all processes running horizontally on the floors(Rehbohm et al., 2022a).

When you walk through the individual floors of the entire building, it becomes clear that an information security officer can handle tasks on more than just one of these floors. Instead, he must be involved in the strategy from the beginning to ensure the organisation's operation. A risk assessment concerns individual assets and must be carried out across divisions or floors. Different security standards can make sense for other assets. Legal framework parameters (compliance) must be considered, and the organizational, personnel and, in particular, technical requirements derived from them must be communicated, governed and monitored on a horizontal level as well as on the individual floors and, last but not least, improved.

11.6 Summary and Conclusion

It was possible to discern a relationship between the role of the CISO in organizations and the awareness of security in these organizations, both in the literature and the studies (surveys). In administrations where there is less awareness of security issues at the

management level, the person responsible for this area is usually subordinate to the IT department. In administrations where there is a greater awareness of the risks of information security and its impact on business operations and the associated external image, the information security officer has greater proximity and independence to the management level. From this, it can be concluded that the role of the information security officer and his role in the administrations studied are directly related to the existing awareness of this issue and that information security is not only an organizational matter but also a social and cultural issue.

To cope with the increasing challenges of digitalization and associated threats from cyberspace on the one hand and the requirements related to the ever-accelerating technological and environmental dynamics on the other, local governments must appropriately integrate an appropriate role into their organizational structure that is fully dedicated to this task, across hierarchies and, above all, sustainably.

The role of the information security officer must be given an appropriate function name to do justice to the prominent function of the role. In addition, despite the tight tariff structure, the administration must understand that strategic tasks must be located at higher hierarchical levels and that people who perform the tasks associated with the role must be grouped accordingly. This also ensures that the management level and other functionaries take the role of the information security officer seriously and take it seriously. It is also necessary to consider the role in the budget with appropriate financial resources.

If this rethinking does not occur in the administration, the "job" of the information security officer will remain a "Sisyphean Job".

PART C – PROCEDURAL MODEL AND SOFTWARE

If you are out to describe the truth,

leave the elegance to the tailor.

Albert Einstein

This thesis section presents the process model and provides insights into the created software prototype.

12 Insights into the procedural model and the supporting software

12.1 Preliminary View

The process model developed is presented below. The development of the process model and the associated software prototype was driven forward in an iterative process, starting with the research idea.

The M24S® software supports the process model with various modules. At its core is the basic module, which is used to set up the respective client, e.g. view settings or user administration (Figure 66).

The ISMS module should also be mentioned. With this module, the 12 steps of the process model can be run through step by step.

The other modules, such as Quick Check, Project Management, Key Performance Indicator (KPI), Statement of Applicability (SoA) and Business Continuity Management (BCM) support the expansion and sustainable operation of the ISMS.

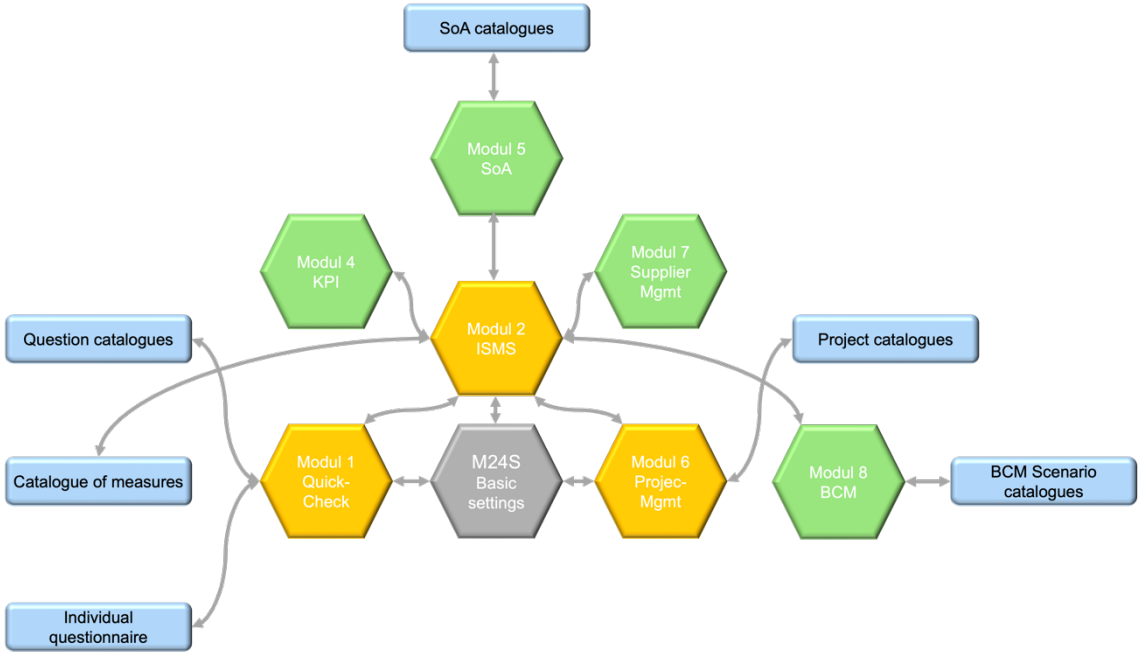

Figure 66: M24S-Modules and Catalogues

To support the client in setting up the ISMS right from the start, M24S provides best practices in the form of template catalogues in the individual steps of the process model.

The process model steps for which one or more template catalogues are available are marked with the symbol below (Figure 67).

Figure 67: Available Catalogues in M24S

This ensures that the process model is open to all systems. Any catalogue of measures (CISIS12, BSI baseline protection, BSI profiles, ISO 27001) can be provided via the software and processed individually or in mixed form as part of the process model. This fact makes it easier for small municipalities to enter the topic of ‘information security’ via BSI profiles and then successively expand the established ISMS.

12.2 Derivation of the individual elements of the process model

In the literature, cyber security is often equated with IT security. However, the increasing digitalisation of administration and the networking of systems and networks makes it clear that an IT-only approach is not expedient. The IT approach can be understood as basic hygiene. It must also be supplemented by personnel, physical and organisational aspects coordinated, controlled and monitored as part of higher-level governance (Bartsch and Frey, 2017, p. 49), (Seckelmann and Brunzel, 2021b, p. 187ff).

Based on the management functions from sections 2.4.2 and 0 and the result of the field experiments, the process model is based on the following five fundamental pillars:

- General Regulations, Organisation and Leadership
- Staff, Documentation and Project Management
- Operation
- Risk Management
- Performance Evaluation, Monitoring and Improvement

These five basic processes drive the twelve steps of the process model via the PDCA cycle, which underpin an organisation's assets (compliance, processes, applications, IT infrastructures and facilities) with appropriate measures to increase the cyber resilience cycle by cycle. The process model and the associated software were developed in an iterative research process using both inductive and deductive elements (Moses and Sandkuhl, 2022), (Moses and Rehbohm, 2022a), (Moses and Rehbohm, 2023d). The prototype derived from induction research, which initially consisted of ten steps, was supplemented by deduction with two further steps, ‘IT service management’ and ‘internal audit’ (Moses and Sandkuhl, 2024a).

With the help of the developed process model and the supporting software, the aim is to structure the essential tasks in such a way that, especially in small administrations, the introduction to the topic of information security succeeds or is simplified by a predefined process and can then be expanded through further PDCA cycles.

The 12 steps of the process model are described below, and insights into the specially developed software are provided (Figure 68).

It is impossible to provide a comprehensive description of all the functions and options of the software here. For this reason, an essential section of each step is listed below and briefly explained.

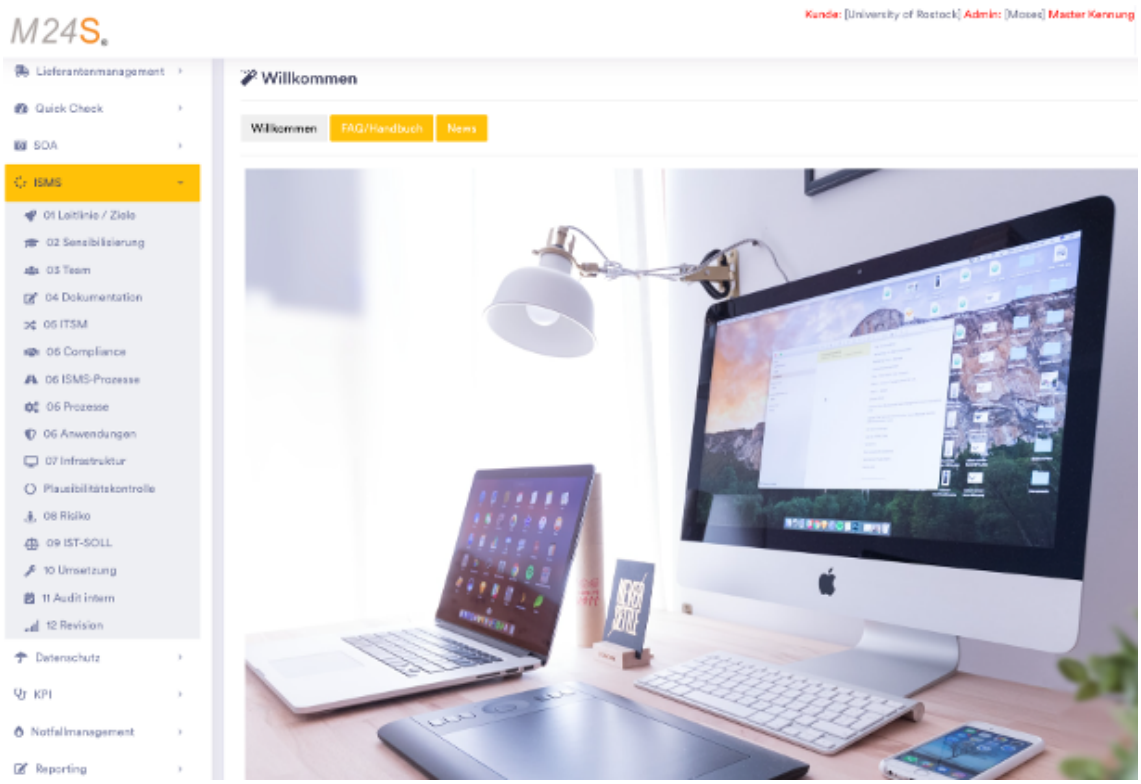

Figure 68: M24S-Software to support the procedural model

12.2.1 General Regulations, Organisation and Leadership

12.2.1.1 Step 1: Policy and Management Attention

When asked which factors hinder the promotion of an information security culture, budget and provability of the benefits, but also management support, are at the top of the list (Rohr, 2015, pp. 403; 414; 466), (Seckelmann and Brunzel, 2021b, p. 187). All three points are symptomatic of information security: the general benefits of information security are difficult to prove, which is why insufficient financial resources are often made available (Seckelmann and Brunzel, 2021b, p. 191). In administrations, in particular, the importance of information security is not recognised at the management level, as information security is often equated with IT tasks (Seckelmann and Brunzel, 2021b, p. 189), (Sowa, 2017, p. 21), (Borum et al., 2015, p. 318).

To ensure awareness at the management level at the start of an ISMS project, the process model suggests in step 1 that an information security guideline be drawn up, objectives defined and agreed with management and then communicated to employees and stakeholders. The recording and monitoring of objectives are supported by selecting ready-made catalogues from M24S (Figure 69).

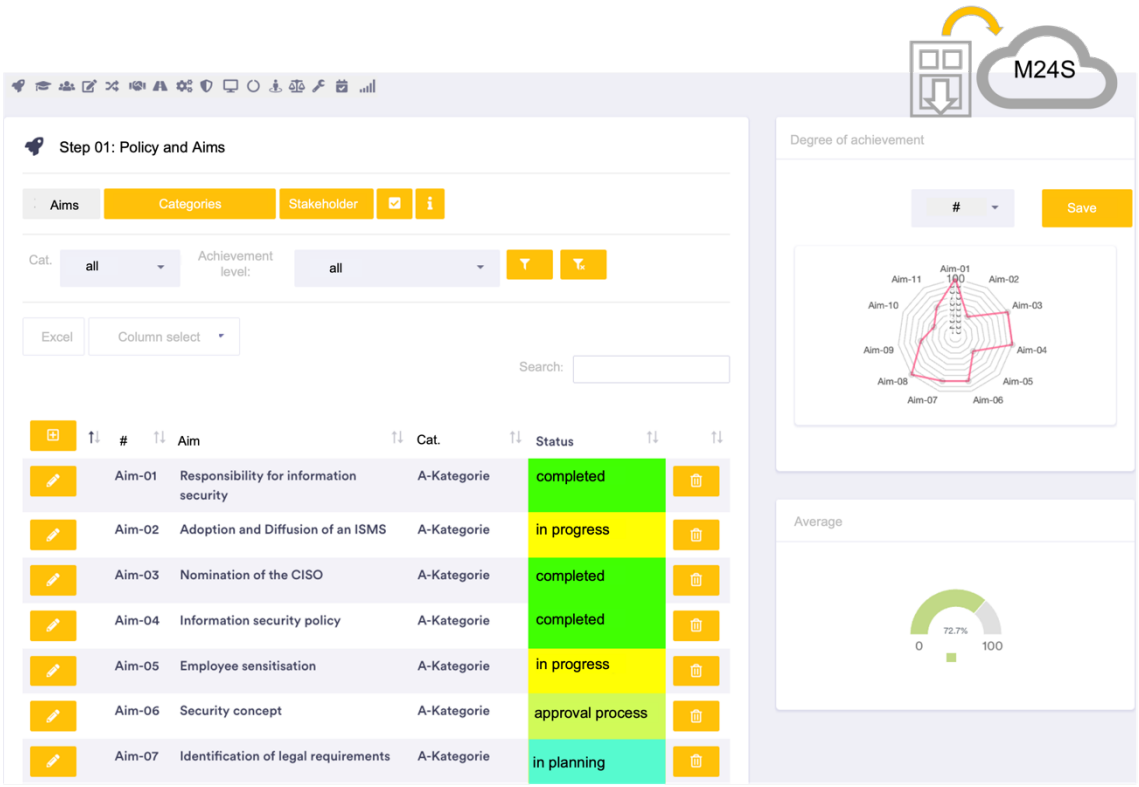

Figure 69: Step 01 - Policy and aims

12.2.1.2 Step 2: Employee awareness and training

Employees are a critical success factor in an information security concept. Employee awareness, i.e. the degree of sensitisation to information security, is therefore an important indicator (Weber et al., 2019, p. 19ff). *Bada* et al. identify five factors that improve the effectiveness of security awareness campaigns: (Bada et al., 2014):

- Professional preparation and organisation
- Do not fuel employees' fears
- Targeted and realisable training content
- Continuously train new behaviours and provide feedback
- Consider cultural specificity and provide target group-specific training

Weber et al. take up these factors and present a 2-phase model with a total of eight activities for employee sensitisation (Weber et al., 2019, p. 21f). *Mohannadi* et al. point out that employee sensitisation should also be extended to IT employees to create sustainable resilience in the organisation (Al-Mohannadi et al., 2018, p. 192).

The software and the process model developed in this work address the need to sensitise employees and place this at the forefront of the process model. This is against the background that even simple personnel measures help to improve information security in an organisation before technical or organisational measures can be implemented with a subsequent review of the degree of implementation.

The M24S software enables users to plan and monitor training measures (Figure 70).

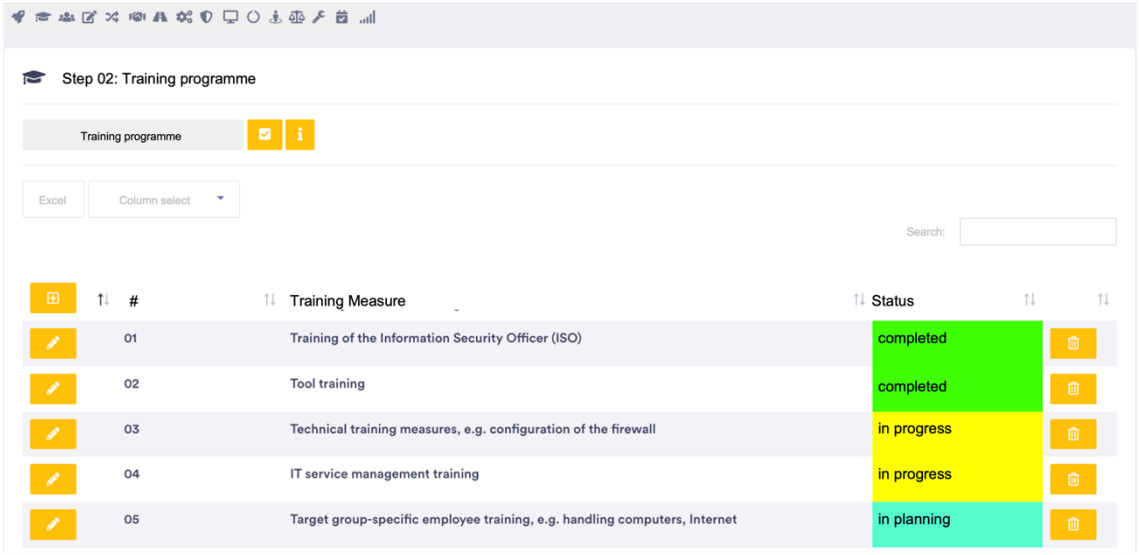

Figure 70: Step 02 - Training programme

12.2.2 Staff, Documentation, Project management

12.2.2.1 Step 3: Team building

The relevant literature assigns significant importance to the ISMS team (Sowa, 2017, p. 2), (Rajivan and Cooke, 2017, p. 203ff), (Jajodia and Albanese, 2017, p. 30ff). *SOWA* provides an overview of the tasks of the ISMS team and, at the same time, describes the team composition and the expertise of the individual team members (Sowa, 2017, p. 26f). *SINLAPANUNTAKUL* et al. identify three competencies that are required to perform independent and collective actions that help to achieve team goals: Attitudes, Behaviours and Knowledge.

Attitudes relate to how team members think about each other, what skills they have to fulfil tasks and what contributions they make to the team (Keebler et al., 2022, p. 253), (Salas et al., 2008, p. 906). **Behaviours** refer to how team members communicate, coordinate and decide to achieve their goals (Keebler et al., 2022, p. 253). **Knowledge** refers to the understanding of team members and strategies used to interpret information (Keebler et al., 2022, p. 253).

Although team competencies are well studied, there is a gap between the available team literature and the literature on cybersecurity teams (Simonson et al., 2020). Team competencies and associated variables provide insight into the limitations of team training currently used in cybersecurity. These limitations include the inability to effectively measure certain competencies and variables in exercises or real-world situations, the lack of variables identified and studied in current cybersecurity team research, and the lack of validated instruments to measure these competencies.

The team building process is supported by M24S (Figure 71). Predefined roles can be assigned to the individual users of the software. This ensures that all essential roles for the

ISMS are assigned to the corresponding employees (Yoo et al., 2020). At the same time, the graphic below serves as an essential information and communication tool.

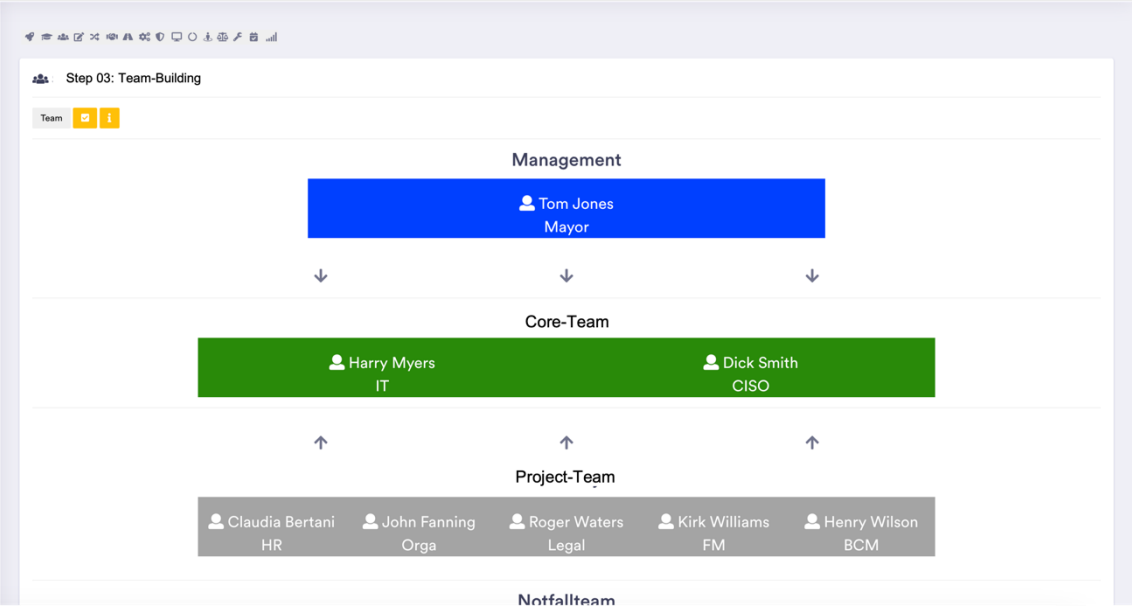

Figure 71: Step 03 – Team building

The requirement formulated above for measuring team competencies can be fulfilled with the help of step 2 "Training programme" of the process model.

12.2.2.2 Step 4: Documentation tasks

Organisations introduce an ISMS to fulfil legal requirements, particularly the General Data Protection Regulation (GDPR), and to protect sensitive information and information structures. One requirement of ISMS is to ensure sufficient (IT) documentation (Kristin Weber et al., 2020).

A significant challenge when using innovative technologies or operating complex IT infrastructures is maintaining an overview of the entire system landscape, business processes, workflows, resources, and risks in complex processes and infrastructures. Appropriate documentation supports goal-orientated action, even in exceptional situations (Reiss, 2018, p. 2).

The ISO 27001 standard defines "documented information" as information that needs to be controlled and maintained by an organisation and the medium on which it is contained (*DIN ISO/IEC 27000*, 2016, p. 11). The (IT) documentation must support all areas of an organisation and provide information for specific target groups (Reiss, 2018, p. 55).

Which part of the (IT) documentation is necessary for an organisation, and in which scope is individual, depending on internal and external organisational conditions and the respective security requirements? *REIS* and *REIS* divide the (IT) documentation into four parts (Figure 72).

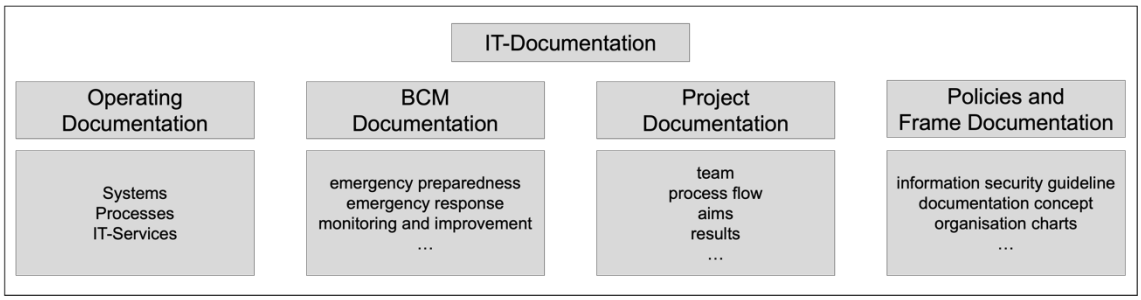

Figure 72: Step 04 - IT-Documentation

Operation documentation includes all documents relating to operational IT operations, i.e., documents required for maintenance and troubleshooting. The Business **Continuity Management** (BCM) documentation describes what to do in the event of an emergency to avert damage to the organization and measures to quickly return to normal operations during emergency operations (Reiss and Reiss, 2018, p. 245; Von Faber and Behnsen, 2018, p. 211). The **project documentation** includes all documents that are created during the project. The **framework documents** comprise all documents that set out guidelines that are valid throughout the organization (Reiss, 2018, p. 55).

The process model requires the creation of appropriate documentation in step 4. The M24S software supports the creation through corresponding template catalogues, which contain the metadata of the necessary documents with a short description of the contents (Figure 73).

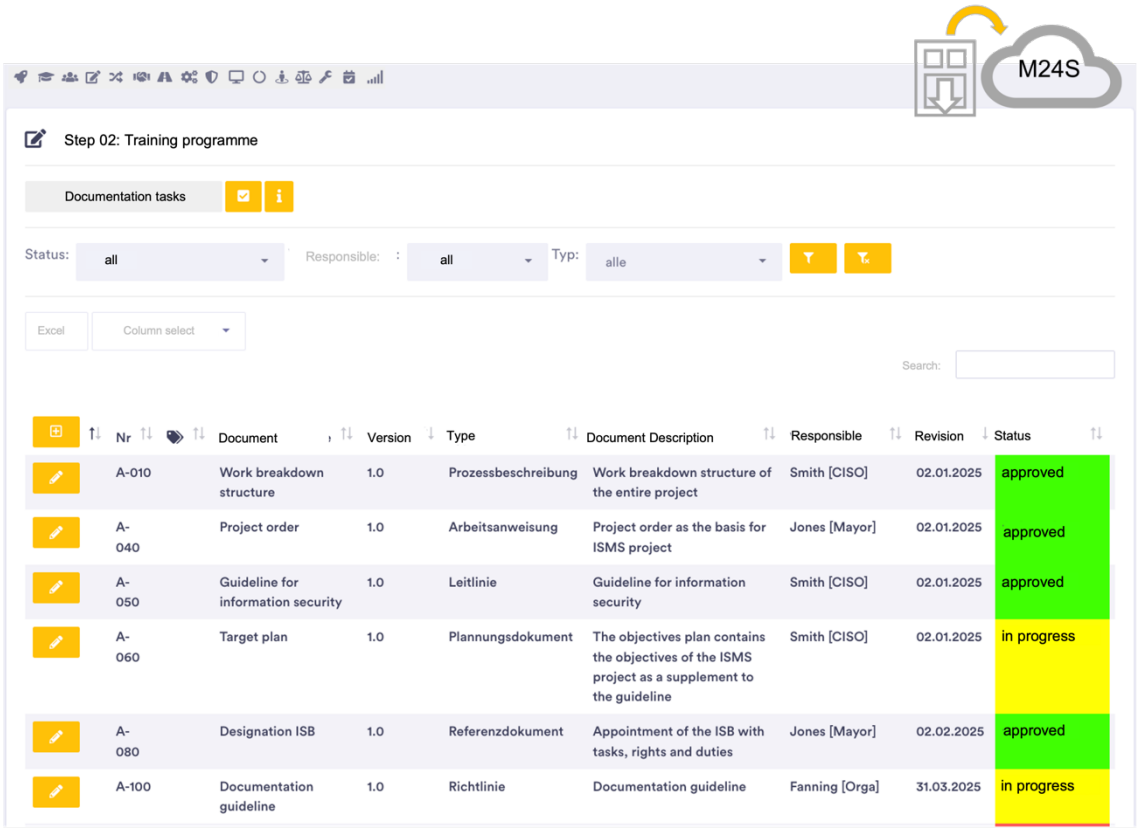

Figure 73: Step 04 - Documentation tasks

12.2.3 Operation

12.2.3.1 Step 5: IT-Service-Management-Processes

The so-called IT Infrastructure Library (ITIL) has been established in IT service management (ITSM). ITIL is a collection of proven methods in ITSM and provides IT service managers with guidelines on implementing professional IT service management (Ebel, 2021, p. 4).

This broad collection of methods is oversized for local authorities (Völker, 2012, p. 18). For this reason, FitSM has become more widespread in recent years as a lightweight framework for SMEs' IT service management (Rohrer and Söllner, 2017). However, in the context of information security, it is sufficient for SMEs to focus on the following three IT services as a first step:

- Maintenance (a predictable process that takes place regularly)
- Change (unpredictable process)
- Incident (unpredictable process due to a sudden event)

Step 5 of the process model focuses on this need for IT service management processes: incident, maintenance and change management (Figure 74).

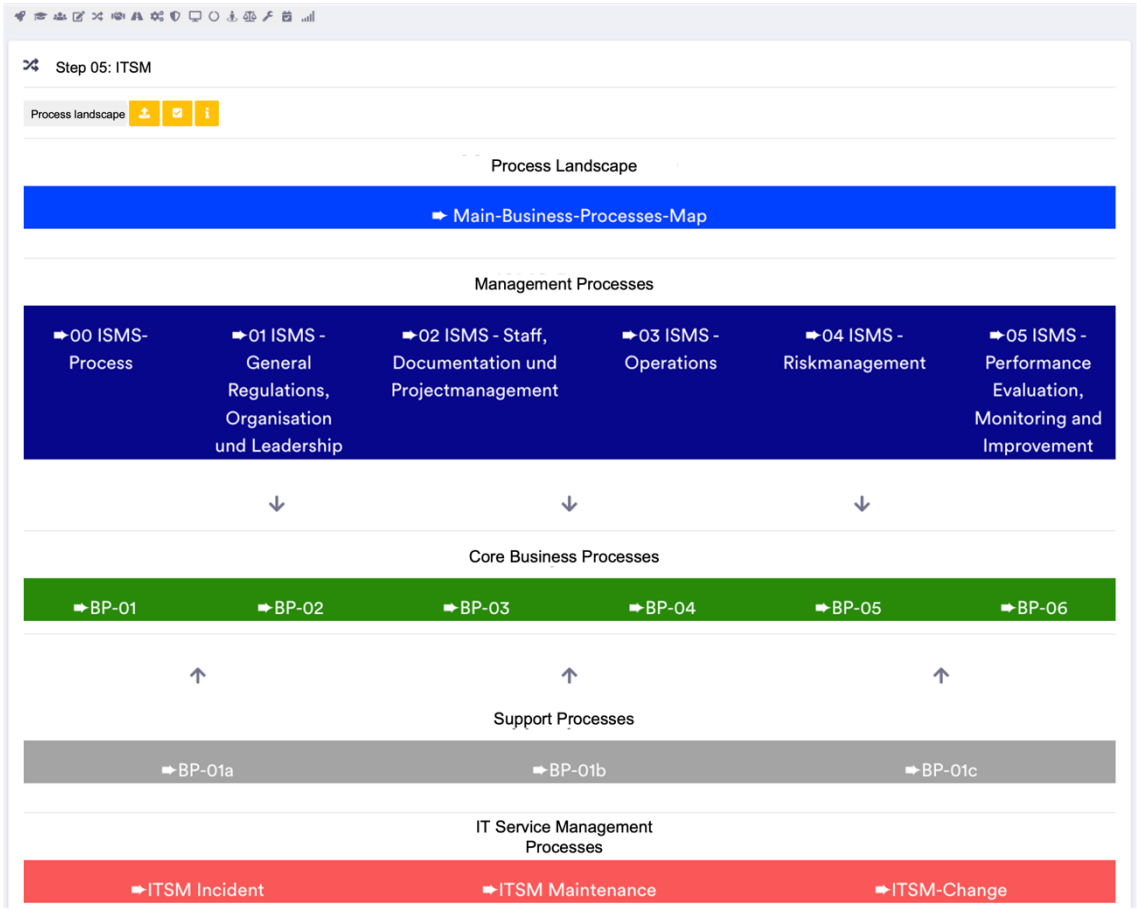

Figure 74: Step 05 - Process Landscape

All processes modelled in M24S are summarised here in a process map, which serves as an information and communication tool.

12.2.3.2 Step 6: Modelling of Compliances, Processes and Applications

Steps 6 and 7 are used to model the information network. Firstly, the scope of the ISMS is defined. Once this has been done, the relevant protection objects, such as processes, applications, IT infrastructures and building,s are identified. The identified assets are assigned relevant security measures (“BSI-Standard 200-1,” 2024, p. 10; “BSI-Standard 200-2: IT-Grundschutz Methodik,” 2024, p. 105). The organisation is responsible for adapting the scope, including the identified assets, appointing those responsible and implementing the measures (Pfeiffer and Seiffert, 2019, p. 25).

The information network can be modelled with the help of M24S. The figure below provides an overview of the identified business processes within the scope (Section 2.1.3), (Figure 75In step 6, the assets compliance, ISMS processes, business processes and applications are recorded and linked together. By connecting them, the need for protection is passed on from the business processes to the applications and subsequently to the IT infrastructure. The criticality of the business processes determines the protection requirements and the desired level of information security (Liedtke, 2022, p. 19).

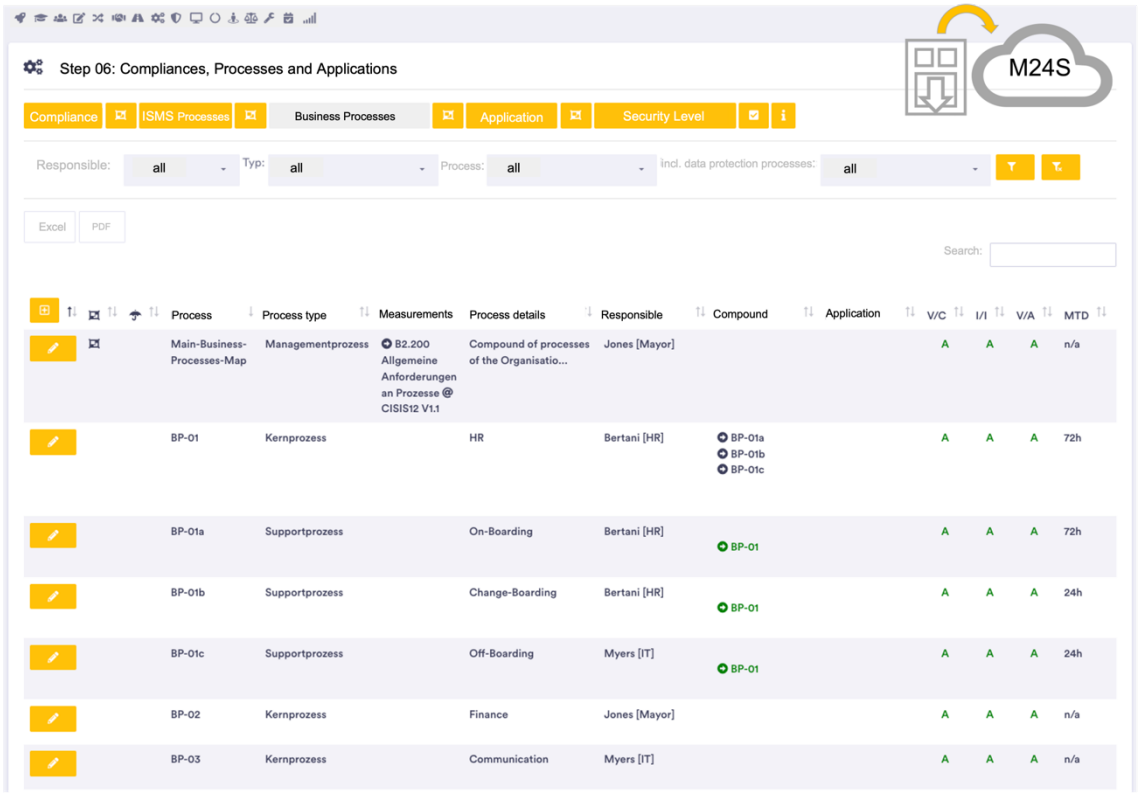

Figure 75: Step 06 - Scope - Business Processes

12.2.3.3 Step 7: Modelling of IT-Infrastructure and Facilities

In principle, there is a free editing option in M24S. However, M24S also provides so-called asset catalogues based on best practices for recording assets (Figure 76).

These asset catalogues contain both the assets and further information regarding the necessary packages of measures for the respective asset. This ensures inexperienced

users can access best practices and subsequently model an information network quickly and easily (Liedtke, 2022, p. 203).

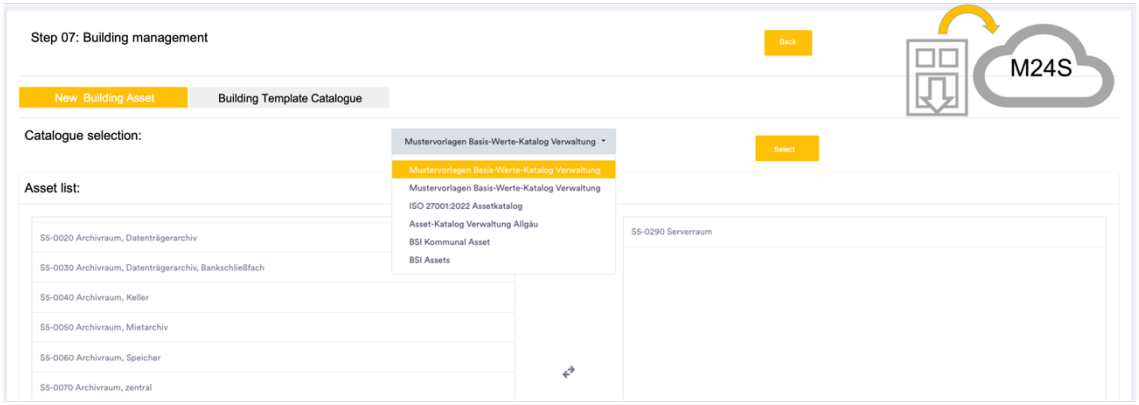

Figure 76: Step 07 - Selecting an Asset from a Catalogue

After selecting the required assets and assigning the measures, M24S provides a corresponding overview (Figure 77).

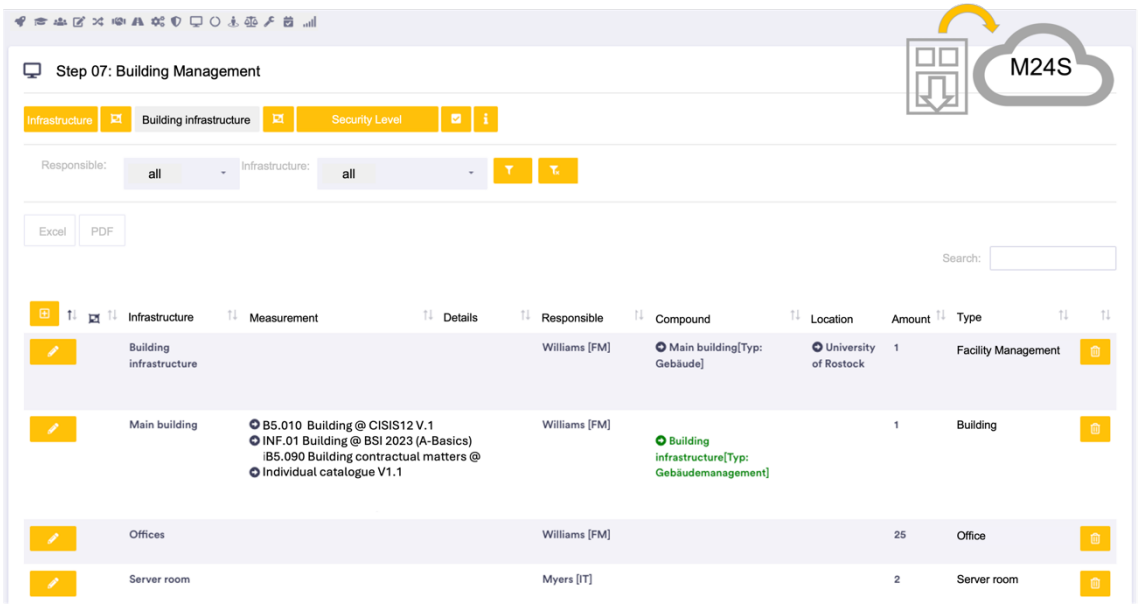

Figure 77: Step 07 - Scope- Buildings

By using different template catalogues and catalogues of measures, M24S can be used to model the respective ISMS according to different objectives:

- Provision of asset and measure catalogues to meet the requirements of CISIS12
- Provision of asset and measure catalogues to meet industry-specific requirements
- Individual adaptations to organisation-specific requirements

Regardless of this, both the process model and the software ensure that an ISMS project can be started ‘small’ and the ISMS can grow step by step (Section 2.1.3). This removes many of the obstacles to setting up an ISMS (Section 9.4.2).

12.2.4 Risk Management

12.2.4.1 Step 8: Risk Management

Due to a lack of personnel and time, risk management is a major challenge for small organisations (Hahn, 2020, p. 7). At the same time, SMEs face the same risks as large organisations but are always more vulnerable due to their fewer resources (Alahmari and Duncan, 2020, p. 2).

In the literature and relevant standards, risk management as a management process is located at the management level of an organisation (Königs, 2017, p. 113), (Moses, 2024, p. 446). In contrast, risk management is the responsibility of the operational departments, as otherwise, the principle of segregation of duties is not guaranteed (Königs, 2017, p. 114).

How risk management should be organised depends on various factors such as size and complexity, operational activities and risk exposure of the organisation as well as human resources (Hunziker and Meissner, 2017, p. 31f). The performance of "information security" is primarily characterised by information security risk management that is aligned with the business strategy and objectives (Königs, 2017, p. 174ff).

Small organisations such as local authorities often have a clear structure and can be managed transparently. In this situation, a simple risk management process in the context of information and cyber security that is integrated into the management structure and the ISMS team is sufficient (Hunziker and Meissner, 2017, p. 32).

The integration of risk management into the process model and in M24S, as an intuitive component, is a critical success factor. In the first step, M24S selects 1-n risks from a risk catalogue for any asset, e.g. Physical Damage - Fire (Figure 78).

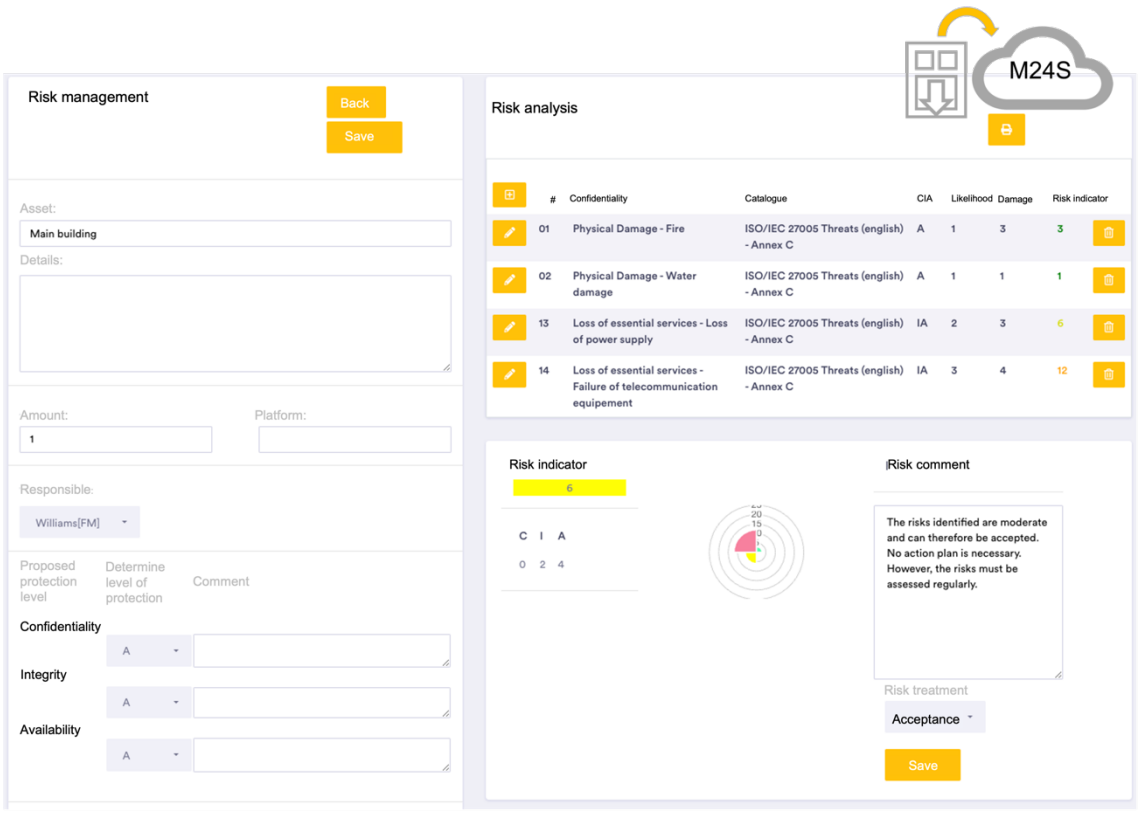

Figure 78: Step 08 - Risk radar of an asset

In the second step, the risk assessment takes place by evaluating the probability of occurrence and the damage for each risk. This can be done by the risk owner alone or as part of a group dynamic process (Figure 79).

Once all the risks of an asset have been assessed, M24S determines a risk indicator for the respective asset. Depending on the level of the risk indicator determined, a risk treatment strategy can then be defined with a corresponding commentary (Figure 78). Here, too, the focus should be on a group-dynamic decision-making process (Moses, 2024, p. 446).

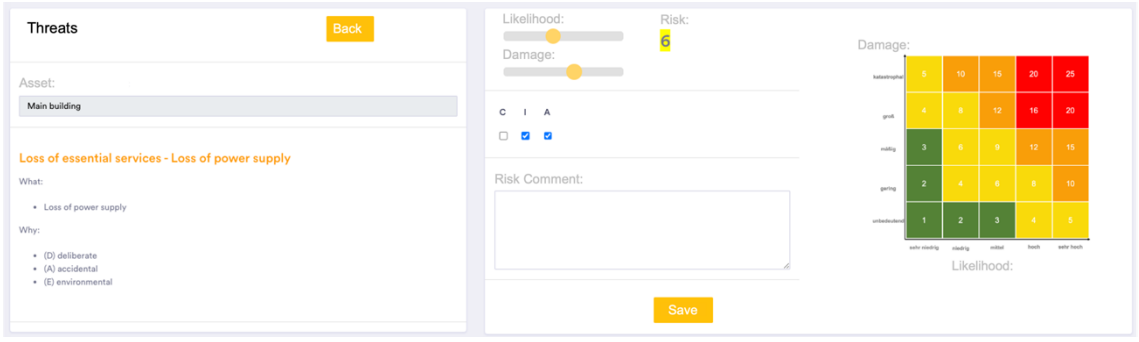

Figure 79: Step 09 - Risk assessment

12.2.4.2 Step 9: Gap-Analyses and Step 10: Planning and Implementation

Once the risk assessment has been completed, it is necessary to check the implementation status of the modelled safety measures. M24S supports this evaluation process (Figure 80). For the selected asset, you can check to what extent the requirement has been implemented (left frame in Figure 80). Depending on the degree of

implementation, implementation planning can be carried out on the right-hand side (the right frame of Figure 80)

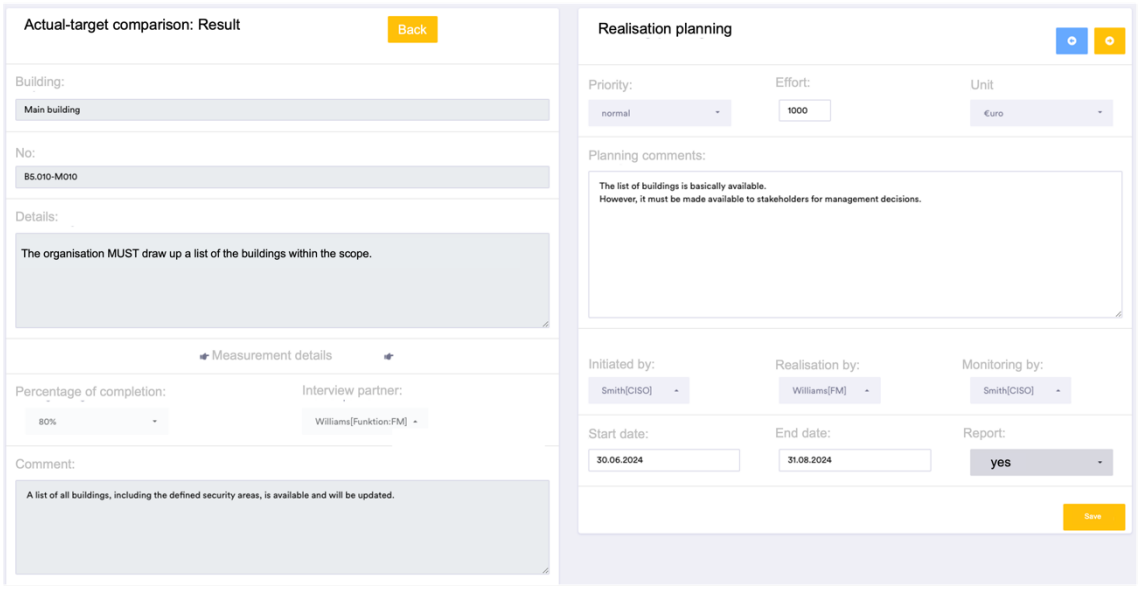

Figure 80: Step 10 - Assessment of actual target

12.2.5 Performance Evaluation, Monitoring and Improvement

12.2.5.1 Step 11: Internal Audit

The primary purpose of audits is to demonstrate or verify conformity to a specific standard (Kersten et al., 2013, p. 76). Conducting an audit is also a way of comparing an actual value with a target value (Kersten et al., 2013, p. 75). Many measures need to be implemented, particularly in the context of information security. This quantity can only be checked with the help of regular spot checks using an internal audit (Hanschke, 2020a, p. 18). The internal audit, therefore, does not focus on the certification of conformity to a standard but rather aims to compare the actual status of specific measures with a target value and to identify the potential for improvement (Kersten et al., 2013, p. 34). The internal audit is, therefore an essential component of an ISMS (Hanschke and Schwarz, 2019, p. 217).

M24S supports creating and implementing an internal audit with the help of standardised questions. The internal audit results are recorded in an audit report (Figure 81).

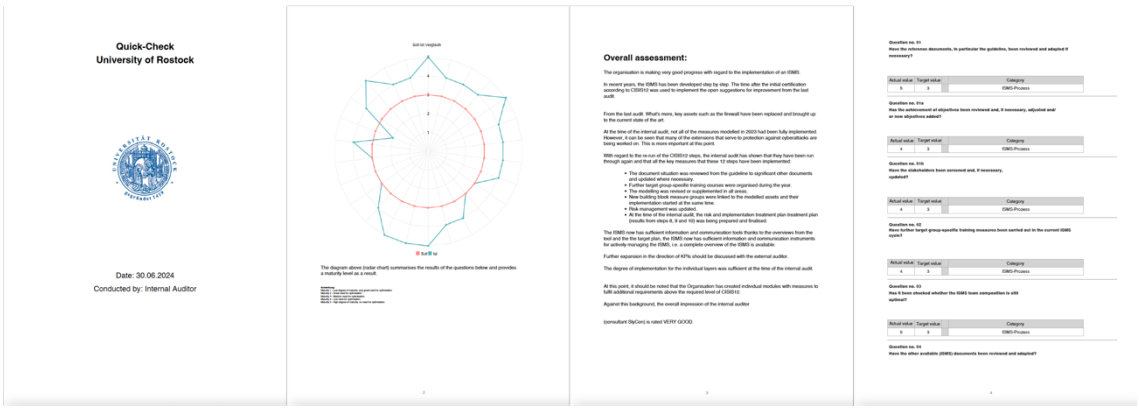

Figure 81: Step 11 - Audit report

12.2.5.2 Step 12: Revision

Setting up and establishing an ISMS is one side of the coin, whereby the aim is not to entirely develop an ISMS as part of the first PDCA cycle. The system-inherent further development occurs as part of further runs of the PDCA cycle (Liedtke, 2022, p. 131). The focus is not just on implementing appropriate security measures or updating documents. The ISMS process itself must be regularly checked for effectiveness and efficiency. This control task should be carried out regularly by the management level and documented through a management review (“BSI-Standard 200-2: IT-Grundschutz Methodik,” 2024, p. 131).

The necessary information is generated as part of the processing of the 11 steps and provided to the stakeholders by M24S as an information and communication tool in the form of a dashboard (Figure 82), (Figure 83).

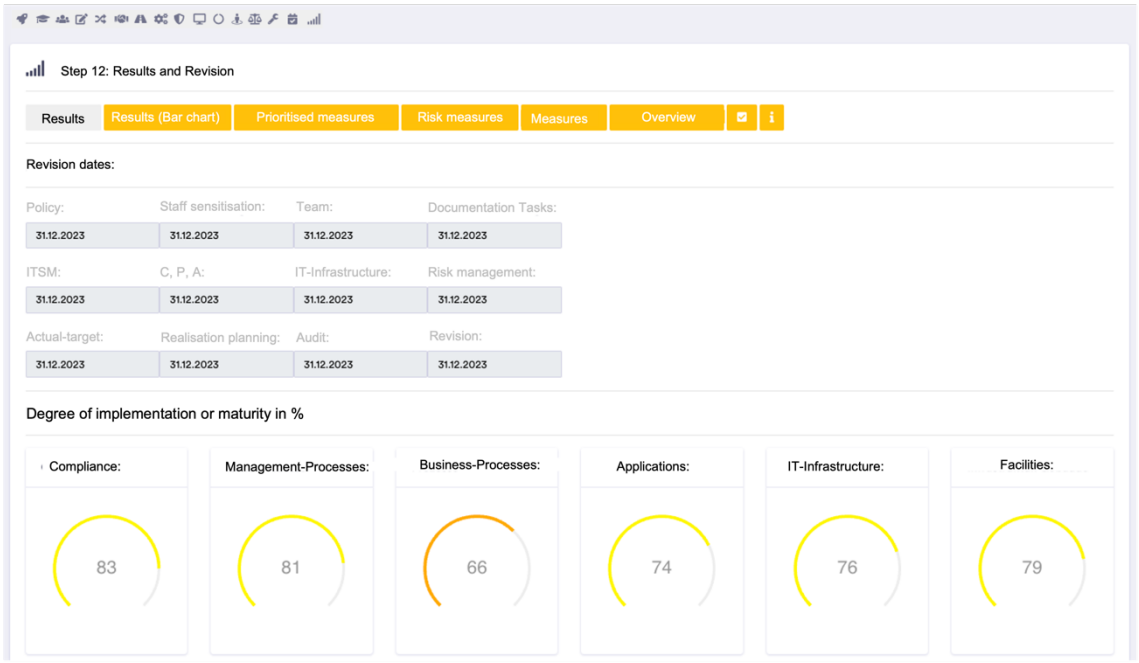

Figure 82: Step 12 - Status quo of the implementation of security measures

The management level needs information in a target group-specific form about the status quo of the ISMS and current decision-making and action requirements to make the right decisions when controlling and steering information security processes (Hanschke, 2020a, p. 73).

The balanced scorecard (BSC) with corresponding KPIs provides an optimal foundation for decision-making processes at the management level to determine how effectively and profitably the measures or investments meet the organisation's overarching objectives (Kaplan, 1999; Onwubiko and Onwubiko, 2019). The figure below provides an insight into possible KPIs (Figure 82).

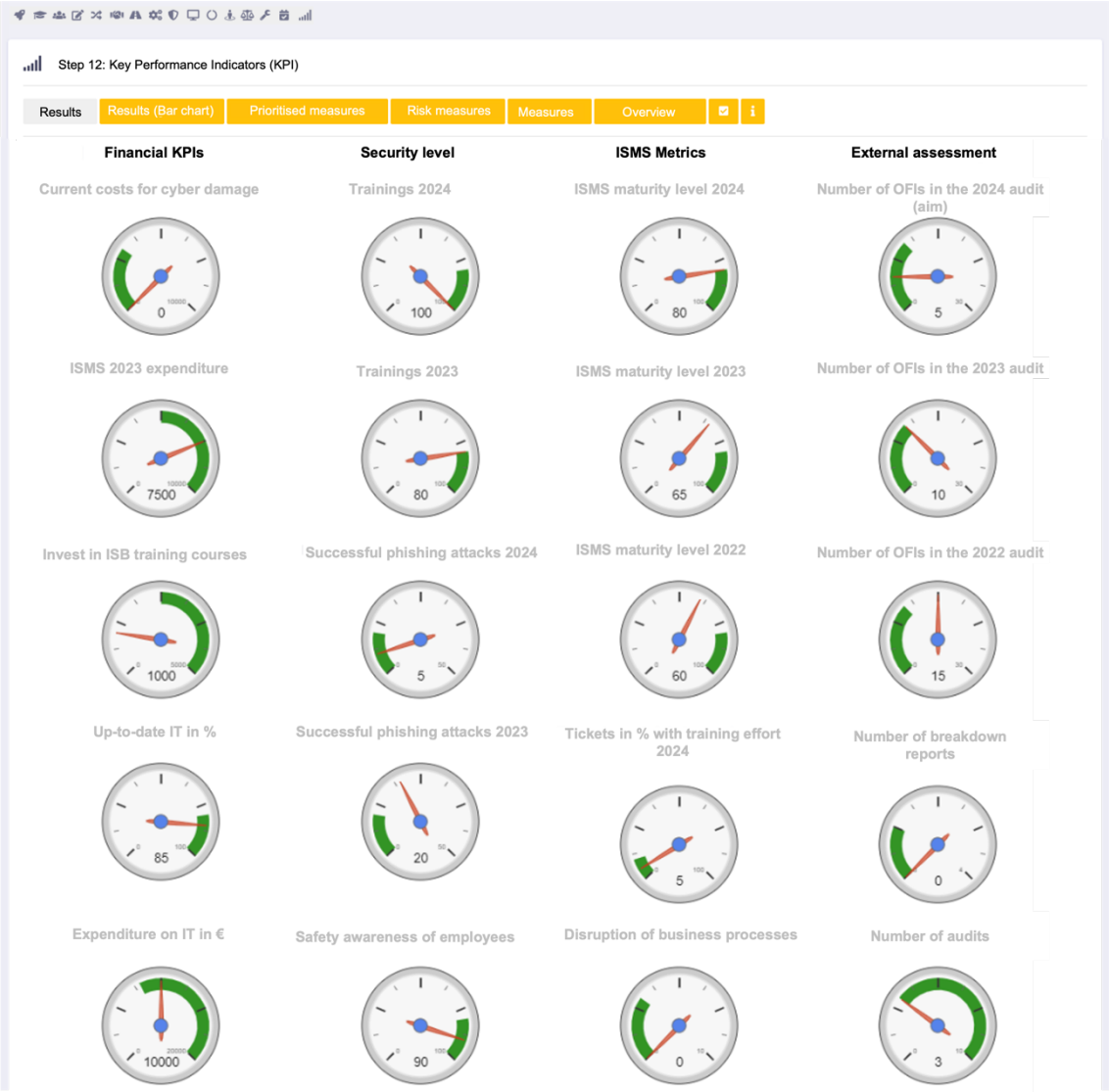

Figure 83: Step 12 - Samples of KPIs of the ISMS

12.3 Summary

With the help of M24S, the twelve steps of the process model are covered, and the user is supported step by step in setting up the ISMS. At the same time, using different catalogues of measures makes it possible to design the ISMS polymorphically. This ensures that the established ISMS can be further developed in different directions, such as ISO 27001 or BSI, or in a hybrid form.

PART D – SUMMARY

Believe you can and you’re halfway there.

Theodore Roosevelt

The last part of the thesis summarizes the results and provides implications for science and practice. Furthermore, it lists the theoretical and practical implications, the applicable limitations and the need for further research.

13 Summary and Outlook

13.1 Discussion the Results

Information security is a significant challenge for small local authorities. However, information security is not one of the core tasks of an administration. It is cost-intensive and places particular demands on staff.

This work is dedicated to this exciting topic, both in practice and science, and thus develops a fundamental understanding of this field of research.

Previous research on information security in the public sector in general and in local government, in particular, has only shed light on partial aspects, such as training and awareness-raising measures or technical security measures. Different requirements are examined in the literature. However, a comprehensive picture of the research area is not drawn.

To address this research gap, various research questions were posed at the beginning of the research project and analysed using multiple scientific methods within the work of this dissertation. The design science approach (DSR) as a research paradigm flanked the research work. This allowed the research problem described in Section "1.1 Problem Definition and Motivation " to be examined more thoroughly. Using the DSR approach, various artefacts were developed and evaluated in this thesis.

The principles described by *HEVNER* et al. and their application are briefly described below:

- **Problem relevance**
  The lack of a process model for setting up and establishing an information security management system could be derived from the literature. Although solutions exist, they cannot be used without a corresponding revision and adaptation to the requirements of the research domain. However, no specific guidelines address the implementation of an ISMS in a small local authority. The results from the analysis of audit reports underpin the lack of a framework and procedure model. This thesis addresses precisely this point and shows how the research problem can be solved with the help of the developed process model and policy framework.
- **Design as an artefact**
  In addition to a process model, a catalogue of measures and a policy framework were developed as a solution approach. The process model is supported by specially designed software.
- **Design evaluation**

From the beginning of the research model, the development of the process model and the software were driven forward in parallel. The prototype process model and the supporting software were subjected to initial laboratory tests to demonstrate their functionality. Subsequently, the evaluation was carried out through field experiments at 24 local governments. From the test under natural conditions, corresponding implications could be derived, and insights could be gained. Despite time and technical and organisational complexity, the field experiments were successfully carried out. This cleared the high hurdle of convincing several local governments to implement an ISMS under scientific supervision. As a result, it was shown that the artefacts have the potential to positively influence the structure of an ISMS.

- **Research contribution**
  In this thesis, the need for research in the development of a process model and its implementation in municipal practice is identified. In addition to the fundamental problem of the willingness of the management level to address the topic of information security, the present work provides a foundation for the holistic treatment of information security management topics.
- **Research rigour**
  Proven methods and constructs from the knowledge base were used to develop the artefacts. These include the methods of TOGAF, as well as the requirements of the BSI Compendium and the requirements of the ISO 27000 family of standards.
- **Design as a search process**
  The consistent use of established and open standards ensures the application and further development of the artefacts. The process model, the software, the policy specifications, and the catalogue of measures are further developed from an optimization point of view, and the results are passed on directly to the user via the SaaS platform.
- **Communication of research**
  The work addresses different target groups. First and foremost, the CISO of an organization is to be addressed. To the same extent, however, the management level of an organization should also be sensitized to the topic. On the one hand, the specifics of the local government, obstacles and success factors are presented, and on the other hand, details on the implementation of an ISMS are presented. To communicate the results, the development and evaluation processes of the artefacts were presented accordingly. In addition, selected aspects of the present artefacts were presented at research conferences. Feedback from the 24 test subjects was also considered in the Design Science Research cycles.

13.2 Theoretical Implications

There has been a gap in previous research regarding a fundamental work on establishing information security management, especially in small local governments (Section 1, 4.3.1).

This thesis has taken up this need and examined the research area of local government and information security from different perspectives (Section 2).

As a result, a procedural model for the research domain of local government was developed, evaluated and presented (Section 4-10). This provided an overall understanding of the conditions and design of the structure of an ISMS in a local government.

Further research can build upon this procedural model and either refine it or apply it to other research contexts. The findings and results can be used in many ways (Section 4.3.2). For example, the data from the modelled IT networks, including the measures used, can be evaluated regarding their benefits and resilience to threats to derive statements for the organisation's future resilience or the measures' sustainable resilience. It is precisely this possibility of making the existing data usable for further evaluation by transferring it to a data warehouse that could enable conclusions to be drawn from the past to the future, which could be very interesting from the point of view of cybersecurity research.

Furthermore, many factors were identified in the study that harm the establishment of an ISMS (Section 9.4.2). Some of these disruptive factors could be eliminated with the present work. For behavioural and personnel research, topics such as employee sensitization or organizational behaviour could be of further interest.

In total, 24 field experiments were carried out in local governments of different sizes (Section 6.5). The experiments provided insights into the natural effect of the developed artefacts on local governments for the first time. However, the findings from the experiments can also be transferred to small and medium-sized companies whose core business is not information security. It can be assumed that the implementation of the process model achieves similar results for SMEs as in the experiments carried out. However, the effectiveness may also vary due to different personnel, financial and organizational conditions.

By using the process model by organizations of different sizes and thus different framework conditions, it could be shown that various organizations use the artefacts developed for the construction of an ISMS in the same way but that the respective personnel, financial and organizational framework conditions still have an impact on the duration of the project or the sustainability of the further implementation. These findings can be used to understand user behaviour better and to research it even further in the future, thus further strengthening resilience.

It is also interesting for science to note that the developed artefacts only achieve the desired effect with a suitable driver (Section 11). Implementing such a project requires external support from a consultant or a responsible person appointed by the organization's

management level, the so-called Chief of Information Security Officer (CISO). The importance of the CISO was accordingly emphasized in this work.

At the same time, the framework parameters of public administration were presented for further research. In particular, behavioural parameters must be considered in order to successfully implement an ISMS project in local governments (Section 2.5).

The results of this work can also be used to further work on the research map in the field of information security in local governments. During the development of the process model, it was possible to show how experts deal with the process model and the software and what effects can be achieved with it (Section 4.3.7).

13.3 Practical Implications

Any administration can benefit from the results of this work. With the help of the developed procedural model, experts can gain a basic understanding of the structure and establishment of an ISMS in a local government.

24 field experiments were carried out in local governments of different sizes. These results can be used to help other local governments get started with information security management.

The cooperation with the 24 municipalities has provided many insights into the municipal landscape. It also quickly became clear that many mayors avoid the sensitive information security topic. Many mayors and members of the management level of local governments were convinced to take up the topic of information security as part of this research work. As a result, the number of local governments that work successfully with the process model has risen to over 250 clients (Section 4.3.6, Status as of August 2024). This made it possible to prove the process model's and the software's functionality.

With the help of these clients and also the existing data, evaluations can be carried out with the help of data warehouse tools to design prediction processes (Section 4.3.5). This allows new measures to be developed and delivered through the SaaS applications that can better withstand future threats, thereby maintaining the resilience of the individual organization in the long term.

While the prototype of the process model and the software were still tested in the laboratory, the field experiments were all carried out under natural conditions. This distinguishes the results of this work and the associated possibilities of use in practice from those of other works. The findings were acquired under natural conditions. In addition, the 24 subjects were supervised for several years (2019-2023) and thus achieved a higher validity and are therefore more transmissible than would be possible through pure laboratory experiments (Section 4.3.4).

In addition, both the clients who have been working with the process model for a long time and the "new" organizations that have only recently started working with the process model were surveyed, and the results of these two groups were compared. This made it possible to create implications integrated into both the process model and the software via the iterative development process (Section 4.3.4).

Furthermore, it could be shown that with the help of a process model adapted to the local government's requirements, the management level's and the employees' willingness to introduce an ISMS of their own accord is growing (Section 4.3.4). The process model presented, and the software application significantly contribute to the last point. On the one hand, this is due to the intuitive operation of the application. On the other hand, the process model makes it possible to implement the philosophy ‘Think big, start small and grow step by step’. This means that small local authorities can approach the topic of information security step by step, taking into account the organisational, technical, personnel and financial parameters that apply there.

The practical reader of this thesis can use the findings to gain a basic understanding of the implementation of an ISMS and thus make his organization more resilient against threats from cyberspace. At the same time, an ISMS can achieve further economies of scale related to efficient and effective IT operations.

As with the theoretical implications, appointing an appropriate person to lead the overall project is a crucial success factor for the practical implications (Section 11). Against this background, this thesis should also make it clear to the reader that not only a process model and a tool contribute to a project's success but also the right team. Without a team and appropriate management attention, establishing an information security management system remains a Sisyphean task, even in small organizations.

13.4 Limitations

Like any scientific work, this dissertation is also subject to various limitations. In the following, the limitations applicable to the present work and publications are described.

First, it should be noted that all literature searches were indexed with special search terms. Although additional forward and backward searches have been performed, it is possible that relevant literature has not been identified. The categorization of literature, as well as the coding of the case studies and expert interviews, was secured by appropriate "cross-check" methods to avoid misinterpretations.

All expert interviews, surveys and evaluations in the context of this thesis were conducted with German-speaking persons from administrations. The literature used is mainly from the Anglo-Saxon language area. A generalization at the international level is, therefore only partially given. Nevertheless, there is a corresponding need to catch up in the German-

speaking world. This is probably because the "small local governments" research field is unattractive.

In developing the process model, the qualitative studies mainly looked at small to medium-sized local governments and could not reach all available experts. Expanding the group of experts to include medium-sized to large local governments could have further exciting implications.

Although the research is in small local governments, some SMEs are now using the process model, including the software. Also, expanding the circle of experts for further research could be helpful.

Finally, several areas were ignored in the context of the research contributions, as they would have gone beyond the scope of this dissertation and were not the focus of consideration. In information security, socio-technical topics such as management attention and employee behaviour should be analyzed through behaviour-oriented research.

13.5 Future Work

Future research should continue to move in this exciting research area, "Information Security in Local Governments," and take up starting points of the limitations described, as the research field is constantly gaining importance.

On the one hand, the process model and the software could be evaluated with further catalogues of measures. This would also make it possible to continue research in other countries.

The results of the evaluations and field experiments carried out could be extended primarily to large administrative organisations. In this way, differences and overlaps could be identified and opened to both research areas.

Future research should also look at how vulnerability analysis can be used to develop more individual security measures through data warehouses or AI and make them available to organizations on time.

A further significant need for research is seen in the research field of organisational behaviour. In addition to a simple and intuitive process model and other tools, the motivation effects must be targeted at the management level. Especially in small local governments, there is a lack of appropriate methods.

APPENDIX

The best way to predict your future is to create it.

Abraham Lincoln

The appendix contains the catalogue of security measures used with the process model and the software. The bibliography is also included.

A.1 CISIS12-Framework

The "Bavarian IT Security Cluster e.V." provides now the framework as well as the catalogue of measures.

Follow the link https://cisis12.de/cisis12-dokumente/ for further information.

A.2 CISIS12-Baustein-Maßnahmen-Katalog (deutsch)

Baustein -Nr	Baustein-Bezeichnung	Ziel
B1.010	Complianceanforderungen	Die Organisation leitet aus vertraglichen, rechtlichen, strukturellen und internen Richtlinien und Vorgaben entsprechende Sicherheitsmaßnahmen ab.
B2.010	Gesamtverantwortung	Die Gesamtverantwortung und Rollen für das Informationssicherheitsmanagement sind festgelegt.
B2.020	Sicherheitsziele und -strategie	Die Sicherheitsziele und Sicherheitsstrategie sind seitens der Leitungsebene fixiert.
B2.030	Informationssicherheitsleitlinie	Eine Informationssicherheitsrichtlinie ist erstellt und angemessen publiziert.
B2.040	Interne Informationssicherheitsbeauftragte	Der Informationssicherheitsbeauftragte ist benannt und ist über seine Aufgaben, Rechte und Pflichten informiert.
B2.050	Externe Informationssicherheitsbeauftragte	Der externe Informationssicherheitsbeauftragte ist benannt und ist über seine Aufgaben, Rechte und Pflichten informiert. Ferner sind Regelungen bzgl. Weisungsrechte vereinbart.
B2.060	Aufbau einer Sicherheitsorganisation	Eine angemessene Sicherheitsorganisation ist aufgebaut.
B2.070	Einbindung der Beschäftigten in den ISMS-Prozess	Die Mitarbeiter sind in die Abläufe und Informationssicherheitsprozesse eingebunden.
B2.080	Einbindung der Informationssicherheit in die Abläufe und Prozesse der Organisation	Die Organisation berücksichtigt bei sämtlichen Abläufen und Prozessen die Informationssicherheit.
B2.090	Erstellung eines Sicherheitskonzepts	Ein für die Organisation angemessenes Sicherheitskonzept ist erstellt.
B2.100	Aufrechterhaltung der Informationssicherheit	Es wurde ein Prozess zur Aufrechterhaltung der Informationssicherheit aufgebaut.
B2.110	Information der Leitungsebene mit Hilfe von Managementberichten bzgl. der Informationssicherheit	Es ist sichergestellt, dass die Leitungsebene regelmäßig über den aktuellen Status der Informationssicherheit informiert wird.
B2.120	Dokumentation der Informationssicherheit und des damit verbundenen Sicherheitsprozesses	Die Dokumentationsaufgabe wird durch die Organisation wahrgenommen. Gleichzeitig erstellt die Organisation entsprechende Nachweise bzgl. der Umsetzung der Sicherheitsprozesse.
B2.130	Aufgaben der Organisation	Die Aufgaben der Organisation sind entsprechenden Verantwortungsträgern zugewiesen.
B2.140	Personalsicherheit	Es ist sichergestellt, dass das Personal in den Sicherheitsprozess integriert wird, sich seiner Verantwortung bewusst ist und Regelungen bei Ende der Beschäftigung bestehen.
B2.150	Berechtigungsmanagement	Die Organisation hat sichergestellt, dass der Zugang, Zutritt und Zugriff zu Lokationen, Gebäuden, Systemen, Anwendungen und Daten durch angemessene Maßnahmen gesichert bzw. berechtigt ist.

Baustein -Nr	Baustein-Bezeichnung	Ziel
B2.160	Risikomanagement	Es wurde ein Prozess zu Identifikation, Bewertung und Behandlung von Risiken in der Organisation aufgebaut und etabliert.
B2.170	Notfallmanagement	Die zur Aufrechterhaltung der Informationssicherheit notwendigen Prozesse wurden in das Notfallmanagement der Organisation integriert.
B2.180	Projektmanagement	Die Umsetzung des Informationssicherheitsmanagementsystems wurde als Projekt realisiert.
B2.190	IT-Servicemanagementprozesse	Die Organisation hat sichergestellt, dass das IT-Servicemanagement angemessene in die Organisation und deren IT-Prozesse eingebunden ist.
B2.200	Allgemeine Anforderungen an Prozesse	Die allgemeinen Anforderungen an Prozesse werden von der Organisation umgesetzt.
B2.210	Verwaltung der Werte	Die Organisation hat die wesentlichen Werte der Organisation identifiziert und entsprechende Verantwortliche zu deren Schutz bestimmt.
B2.220	Informationsklassifizierung	Es ist sichergestellt, dass für Informationen ein angemessenes Schutzniveau ermittelt wurde und Informationen entsprechend klassifiziert sind.
B2.230	Dokumentationsprozess und Dokumentlenkung	Der gesamte Informationssicherheitsprozess ist dokumentiert und entsprechend gelenkt.
B2.240	Administrationssaufgaben	Die administrativen Aufgaben sind entsprechenden Verantwortlichen zugewiesen.
B2.250	Patch- und Änderungsmanagement	Der ordnungsgemäße und sichere Betrieb von Systemen und Anwendungen ist durch regelmäßige Updates sichergestellt.
B2.260	Virenschutz	Systeme, Anwendungen und Daten sind vor Schadsoftware angemessen geschützt.
B2.270	Datensicherung	Die Organisation stellt sicher, dass Daten vor Verlust geschützt sind.
B2.280	Datenschutz	Die Einhaltung von rechtlichen Vorgaben insbesondere von (personenbezogenen) Daten ist sichergestellt.
B2.290	Kryptografische Maßnahmen	Es werden angemessene und wirksame kryptografische Verfahren zum Schutz der Vertraulichkeit und Integrität von Daten in der Organisation eingesetzt.
B2.300	Outsourcing (Nutzung)	Das Outsourcing von Diensten oder Anwendungen ist sowohl technisch als auch organisatorisch und rechtlich abgesichert.
B2.310	Nutzung von Cloud-Diensten	Die Nutzung von Cloud-Diensten ist mit entsprechenden Maßnahmen sowohl technisch als auch organisatorisch und rechtlich abgesichert.
B2.320	Löschen und Vernichtung	Die sichere Vernichtung von Daten und Datenträgern ist durch angemessene Maßnahmen sichergestellt.

Baustein -Nr	Baustein-Bezeichnung	Ziel
B2.330	Fernwartung	Fernwartungszugriffe bzw. -zugänge sind durch geeignete technische Maßnahmen abgesichert, so dass zu keinem Zeitpunkt eine Gefahr für die Organisation, deren Systeme, Anwendungen oder Daten besteht.
B2.340	Telearbeit	Es ist sichergestellt, dass sowohl für die Telearbeit als auch der Nutzung von mobilen Endgeräten die Informationssicherheit berücksichtigt und eingehalten wird.
B2.350	Home-Office	Das Home-Office erfüllt die Anforderungen der Informationssicherheit und rechtlicher Rahmenbedingungen.
B2.360	Softwareentwicklung	Bei der Softwareentwicklung werden einerseits die Informationssicherheit im Entwicklungsprozess berücksichtigt als auch andererseits die Vorgaben der EU-DSGVO (privacy by design und privacy bei default).
B2.370	Lieferantenmanagement	Die Organisation stellt sicher, dass sich Lieferantenbeziehungen nicht negativ auf die Informationssicherheit auswirken.
B2.380	Handhabung von Sicherheitsvorfällen	Es ist ein Prozess für die Handhabung von Informationssicherheitsvorfällen einschließlich einer Benachrichtigung von interessierten Parteien etabliert und kommuniziert.
B2.390	Interne und externe Audits	Der Status des Informationssicherheitsmanagementsystem e wird in regelmäßigen Abständen überprüft.
B3.010	Allgemeine Anforderungen an Anwendungen	Die allgemeinen Anforderungen an Anwendungen werden von der Organisation umgesetzt.
B3.020	Virtualisierungsplattformen	Virtualisierungsplattformen werden als Basis für andere Systeme sicher betrieben.
B3.030	Datenbankanwendungen	Der sichere Betrieb von Datenbankanwendungen ist sichergestellt.
B3.040	Kommunikationssysteme (E-Mail-Server, Groupware)	Kommunikationssysteme werden sicher betrieben und sind entsprechend abgesichert.
B3.050	Verzeichnisdienst	Zentrale Dienste werden sicher betrieben.
B3.060	Nutzung von Dokumentenmanagementsysteme n	Die Nutzung von Dokumentenmanagementsystemen entspricht sicherheitstechnischen Vorgaben und die Integrität und Vertraulichkeit der darin gespeicherten Daten ist sichergesellt sowie die Verfügbarkeit per se.
B3.070	Nutzung von Webanwendungen	Die Nutzung von Webanwendungen ist durch angemessene technische und organisatorische Maßnahmen abgesichert und die mit der Webanwendung verarbeitenden Daten in Sachen Integrität und Vertraulichkeit geschützt.
B3.080	Geschäftsanwendungen	Die Organisation hat sichergestellt, dass Geschäftsanwendungen sicher betrieben werden und informationstechnische und

Baustein -Nr	Baustein-Bezeichnung	Ziel
		rechtliche Vorgaben in Bezug auf die Datenverarbeitung eingehalten werden.
B3.090	Bürokommunikationsanwendung (Office)	Es ist sichergestellt, dass Bürokommunikationssysteme sicher betrieben werden und die rechtlichen Anforderungen bzgl. des Betriebes berücksichtigt werden.
B3.100	Betriebssysteme (Client und Server)	Die Organisation stellt sicher, dass Betriebssysteme durch entsprechende Prozesse aktuell und sicher gehalten werden.
B3.110	Web- und Videokonferenzsysteme	Die Nutzung von Web- und Videokonferenzsystemen ist nach rechtlichen und sicherheitstechnischen Vorgaben abgesichert.
B3.120	Zugangs- und Zutrittssysteme	Der unbefugte Zutritt zu Sicherheitsbereichen ist sichergestellt.
B3.130	Nutzung von Cloud-Storage	Die Nutzung von Cloud-Storage ist sowohl rechtlich als auch informationssicherheitstechnisch bzw. organisatorisch abgesichert.
B3.140	MDM	Die Informationssicherheit ist für mobile Endgeräte sichergestellt.
B3.150	VoIP	Beim Einsatz von VoIP werden sicherheitstechnische Rahmenparameter berücksichtigt.
B3.160	Telefonanlage VoIP (PBX) ausgelagert	Die Nutzung von ausgelagerten Telekommunikationsservices sind sowohl rechtlich als auch informationssicherheitstechnisch durch angemessene Maßnahmen abgesichert.
B4.010	Allgemeiner Server	Der allgemeine Betrieb von Serverinfrastrukturen ist durch geeignete Maßnahmen abgesichert.
B4.020	Server (physikalisch)	Die Betriebssicherheit als auch die Informationssicherheit ist für Server sichergestellt.
B4.030	Server für Virtualisierungsplattformen	Die Betriebssicherheit als auch die Informationssicherheit ist für zentrale Virtualisierungsplattformen sichergestellt.
B4.040	Server (virtuell)	Der Betrieb von virtuellen Servern auf Virtualisierungsplattformen ist durch geeignete Maßnahmen sichergestellt.
B4.050	Terminalserver	Der sichere Betrieb von Terminalservern ist sichergestellt.
B4.060	Linux Server	Der sichere Betrieb von Linux-Servern ist sichergestellt.
B4.070	Datenbankserver	Der Bereitstellung von Daten von Datenbankservern für andere Anwendungen oder Server ist sichergestellt.
B4.080	Client (Allgemein)	Die Betriebsbereitschaft von Clients ist sichergestellt.
B4.090	Laptop / Notebook	Die Betriebsbereitschaft von Notebooks ist sichergestellt.

Baustein -Nr	Baustein-Bezeichnung	Ziel
B4.100	Netz- und Systemmanagement	Die Organisation stellt die Administration des Netzwerkes und der damit verbundenen Komponenten sicher.
B4.110	Firewallsysteme	Systeme, Anwendungen und Daten sind vor Schadsoftware geschützt.
B4.120	Router und Switches	Der sichere Betrieb von aktiven Netzkomponenten ist durch technische und organisatorische Maßnahmen sichergestellt.
B4.130	LAN	Der Schutz von Daten in Netzwerken und den damit verbundenen Komponenten ist sichergestellt.
B4.140	WLAN	Der Schutz von Daten in Funknetzwerken und den damit verbundenen Komponenten ist durch angemessene technische und organisatorische Maßnahmen sichergestellt.
B4.150	VPN	Die Kommunikation zwischen den zentralen Systemen und Systemen außerhalb der Organisation ist durch geeignete Netzkopplungselemente geschützt.
B4.160	Speichersysteme	Der Betrieb und Schutz von zentralen Speichersystemen und damit verbundenen Komponenten ist sichergestellt.
B4.170	TK-Anlage (physisch, virtuell)	Die Betriebsbereitschaft der TK-Anlage ist sichergestellt.
B4.180	Druck- und Multifunktionsgeräte	Die Betriebsbereitschaft von Druck- und Multifunktionsgeräten ist sowohl durch technische als auch organisatorische Maßnahmen sichergestellt.
B4.190	Mobilgeräte	Der sichere Betrieb und die sichere Nutzung von Mobilgeräten ist gewährleistet.
B4.200	Fax-Geräte	Die Organisation stellt sicher, dass Fax-Geräte sicher betrieben und genutzt werden.
B4.210	Fax-Server	Die Nutzung von Fax-Servern ist durch angemessene technische und organisatorische Maßnahmen sichergestellt.
B4.220	Legacy-Systeme	Die Organisation stellt sicher, dass Legacy-Systeme sicher weiter betrieben oder inkl. der Datenbestände migriert werden.
B5.010	Gebäude	Der unbefugte Zutritt zu Gebäudeteilen als auch die Gebäude selbst sind angemessenen geschützt.
B5.020	Allgemeine Räume	Büros und sonstige Infrastrukturen der Organisation sind gegen unbefugten Zutritt und Zugang geschützt.
B5.030	Büroräume	Die Büroräume verfügen über die notwendigen Sicherheitseinrichtungen.
B5.040	Funktionsraum (Schulung, Besprechung)	Besondere Infrastrukturen der Organisation sind gegen unbefugten Zutritt und Zugang geschützt.
B5.050	Serverraum	Besondere Infrastrukturen der Organisation sind gegen unbefugten Zutritt und Zugang geschützt.
B5.060	Infrastrukturraum	Besondere Infrastrukturen der Organisation sind gegen unbefugten Zutritt und Zugang geschützt.

Baustein -Nr	Baustein-Bezeichnung	Ziel
B5.070	Mobiler Arbeitsplatz	Mobile Arbeitsplätze erfüllen die Anforderungen der Informationssicherheit.
B5.080	Home-Office	Home-Office-Arbeitsplätze erfüllen ein Mindestmaß an Sicherheit.
B5.090	Archivraum	Besondere Infrastrukturen der Organisation sind gegen unbefugten Zutritt und Zugang geschützt.
iBX.XYZ	Individuelle Bausteine	Individuelle bzw. zusätzliche Bausteine sind von der Organisation erstellt und werden angewendet.

A.3 CISIS12-Catalogue of Modules and Measurements (english)

Module-Nr	Module	Aim
B1.010	Compliance Requirements	The organization derives appropriate security measures from contractual, legal, structural and internal guidelines and specifications.
B2.010	Responsibility	Overall responsibilities and roles for information security management are defined.
B2.020	Security Objectives and Strategy	The security goals and security strategy are fixed by the management level.
B2.030	Information Security Guideline	An information security guideline has been drawn up and appropriately published.
B2.040	Information Security Officer	The information security officer is appointed and is informed about his duties, rights and obligations.
B2.050	External Information Security Officer	The external information security officer is appointed and is informed about his duties, rights and obligations. In addition, regulations regarding the right to issue instructions have been agreed.
B2.060	Establishment of a security organization	An appropriate security organization is in place.
B2.070	Involvement of employees in the ISMS process	Employees are involved in the procedures and information security processes.
B2.080	Integration of information security into the procedures and processes of the organization	The organization takes information security into account in all procedures and processes.
B2.090	Creation of a security concept	A security concept that is appropriate for the organization has been drawn up.
B2.100	Maintaining information security	A process for maintaining information security has been established.
B2.110	Informing the management level with the help of management reports regarding information security	It is ensured that the management level is regularly informed about the current status of information security.
B2.120	Documentation of information security and the associated security process	The documentation task is carried out by the organization. At the same time, the organization prepares appropriate evidence regarding the implementation of security processes.
B2.130	Tasks of the organization	The tasks of the organization are assigned to appropriate responsible persons.
B2.140	Personnel security	It is ensured that staff are integrated into the safety process, are aware of their responsibilities and that regulations are in place at the end of employment.
B2.150	Authorization Management	The organization has ensured that access to locations, buildings, systems, applications, and data is secured or authorized by appropriate measures.
B2.160	Risk Management	A process for identifying, assessing and dealing with risks in the organization was established.
B2.170	Business Continuity Management	The processes necessary to maintain information security have been integrated into the organization's emergency management.

Module-Nr	Module	Aim
B2.180	Project Management	The implementation of the information security management system was realized as a project.
B2.190	IT Service Management Processes	The organization has ensured that IT service management is appropriately integrated into the organization and its IT processes.
B2.200	General requirements for processes	The general requirements for processes are implemented by the organization.
B2.210	Asset Management	The organization has identified the organization's core values and designated appropriate leaders to protect them.
B2.220	Information Classification	It is ensured that an adequate level of protection has been identified for information and that information is classified accordingly.
B2.230	Documentation process and Document Control	The entire information security process is documented and managed accordingly.
B2.240	Administrative tasks	The administrative tasks are assigned to the appropriate responsible persons.
B2.250	Patch and Change Management	The proper and secure operation of systems and applications is ensured by regular updates.
B2.260	Virus protection	Systems, applications, and data are adequately protected against malware.
B2.270	Backup	The organization ensures that data is protected from loss.
B2.280	Data Protection	Compliance with legal requirements, in particular with regard to (personal) data, is ensured.
B2.290	Cryptographic measures	Appropriate and effective cryptographic procedures are used to protect the confidentiality and integrity of data in the organization.
B2.300	Outsourcing (Use)	The outsourcing of services or applications is technically as well as organizationally and legally secured.
B2.310	Use of cloud services	The use of cloud services is technically as well as organizationally and legally secured with appropriate measures.
B2.320	Deletion and destruction	The secure destruction of data and data carriers is ensured by appropriate measures.
B2.330	Remote maintenance	Remote maintenance access is secured by appropriate technical measures, so that there is no danger to the organization, its systems, applications or data at any time.
B2.340	Telecommuting	It is ensured that information security is taken into account and complied with both for teleworking and the use of mobile devices.
B2.350	Home-Office	The home office meets the requirements of information security and legal framework conditions.
B2.360	Software development	In software development, information security is taken into account in the development process on the one hand, and the requirements of the EU GDPR (privacy by design and privacy by default) on the other).
B2.370	Supplier management	The organization ensures that supplier relationships do not negatively impact information security.

Module-Nr	Module	Aim
B2.380	Security Incident Handling	It is established and communicated a process for handling information security incidents including notification of interested parties.
B2.390	Internal and external audits	The status of the information security management system is reviewed at regular intervals.
B3.010	General Application Requirements	The general requirements for applications are implemented by the organization.
B3.020	Virtualization Platforms	Virtualization platforms are operated securely as the basis for other systems.
B3.030	Database Applications	The secure operation of database applications is ensured.
B3.040	Communications (E-Mail-Server, Groupware)	Communication systems are operated securely and are correspondingly secured.
B3.050	Directory service	Central services are operated securely.
B3.060	Use of document management systems	The use of document management systems complies with security requirements and the integrity and confidentiality of the data stored in them is ensured, as well as the availability.
B3.070	Use of web applications	The use of web applications is secured by appropriate technical and organizational measures and the data processed with the web application is protected in terms of integrity and confidentiality.
B3.080	Business Applications	The organization has ensured that business applications are operated securely and that information technology and legal requirements regarding data processing are complied with.
B3.090	Office communication application (Office)	It is ensured that office communication systems are operated securely and that the legal requirements regarding operation are taken into account.
B3.100	Operating systems (Client and Server)	The organization ensures that operating systems are kept up-to-date and secure through appropriate processes.
B3.110	Web & Video Conferencing Systems	The use of web and video conferencing systems is secured in accordance with legal and security requirements.
B3.120	Access Systems	Unauthorized access to security restricted areas is ensured.
B3.130	Leveraging Cloud Storage	The use of cloud storage is secured both legally and in terms of information security and organization.
B3.140	MDM	Information security is ensured for mobile devices.
B3.150	VoIP	When using VoIP, safety-related framework parameters are taken into account.
B3.160	VoIP (PBX)	The use of outsourced telecommunications services is secured by appropriate measures, both legally and in terms of information security.
B4.010	Server	The general operation of server infrastructures is secured by appropriate measures.
B4.020	Server (physical)	Operational security as well as information security is ensured for servers.

Module-Nr	Module	Aim
B4.030	Server for Virtualization Platforms	Operational security as well as information security is ensured for central virtualization platforms.
B4.040	Server (virtuell)	The operation of virtual servers on virtualization platforms is ensured by appropriate measures.
B4.050	Terminal server	The secure operation of terminal servers is ensured.
B4.060	Linux Server	The secure operation of Linux servers is ensured.
B4.070	Database server	The provision of data from database servers to other applications or servers is ensured.
B4.080	Client	The operational readiness of clients is ensured.
B4.090	Laptop / Notebook	The operational readiness of notebooks is ensured.
B4.100	Network and system management	The organization ensures the administration of the network and the associated components.
B4.110	Firewall systems	Systems, applications and data are protected from malware.
B4.120	Router and Switches	The safe operation of active network components is ensured by technical and organizational measures.
B4.130	LAN	The protection of data in networks and the associated components is ensured.
B4.140	WLAN	The protection of data in wireless networks and the associated components is ensured by appropriate technical and organizational measures.
B4.150	VPN	Communication between the central systems and systems outside the organization is protected by appropriate network interconnection elements.
B4.160	Storage	The operation and protection of central storage systems and associated components is ensured.
B4.170	PBX (physical, virtual)	The operational readiness of the PBX is ensured.
B4.180	Printing & Multifunction Devices	The operational readiness of pressure and multifunctional devices is ensured by both technical and organizational measures.
B4.190	Mobile Devices	The safe operation and use of mobile devices is ensured.
B4.200	Fax Machines	The organization ensures that fax machines are operated and used safely.
B4.210	Fax Server	The use of fax servers is ensured by appropriate technical and organizational measures.
B4.220	Legacy systems	The organization ensures that legacy systems continue to be operated securely or migrated including data assets.
B5.010	Building	Unauthorized access to parts of the building as well as the buildings themselves are adequately protected.
B5.020	General Rooms	Offices and other infrastructure of the organization are protected against unauthorized entry and access.
B5.030	Offices	The offices are equipped with the necessary safety equipment.

Module-Nr	Module	Aim
B5.040	Functional room (Training, Meeting)	Special infrastructures of the organization are protected against unauthorized access.
B5.050	Server room	Special infrastructures of the organization are protected against unauthorized access.
B5.060	Infrastructure room	Special infrastructures of the organization are protected against unauthorized access.
B5.070	Mobile workplace	Mobile workstations meet the requirements of information security.
B5.080	Home-Office	Home office workplaces meet a minimum level of security.
B5.090	Archive room	Special infrastructures of the organization are protected against unauthorized access.
iBX.XYZ	Individual Modules	Individual or additional building blocks are created by the organization and are applied.

A.4 Contribution in Publications

The following paragraphs describe the contributions of the authors' thesis to each of the included peer-reviewed publications.

#	Title	Reference / Publishing body	Acceptance Rate / Ranking
1	Empirical Study on the State of Practice of Information Security Management in Local Government **(Section 5)**	**(Moses et al., 2022a)** Moses, F., Sandkuhl, K., Kemmerich, T., 2022a. Empirical Study on the State of Practice of Information Security Management in Local Government, in: Zimmermann, A., Howlett, R.J., Jain, L.C. (Eds.), Human Centred Intelligent Systems, Smart Innovation, Systems and Technologies. Springer Nature, Singapore, pp. 13–25. https://doi.org/10.1007/978-981-19-3455-1_2	**28% acceptance rate**
Contribution	I designed and led the literature analysis for this article. As the author of the publication, I designed and compiled the structure of the paper. The paper was based on an analysis of 421 audit reports on the one hand and an interview study with 50 questions on the other. I planned and conducted the analysis of the audit reports. These results were incorporated into the interview study. I incorporated the recommendations of the two co-authors into the paper.		
2	CISIS12	**(Moses and Rehbohm, 2022a)** Moses, F., Rehbohm, T., 2022. CISIS12. kes, CISIS12.	**Not available**
Contribution	This paper is based on a first draft of a prototypical process model as well as supporting software. Both were developed by me. For the development of the process model, I reviewed the relevant literature and discussed the status quo of research. My contribution in this publication is the literature research and the chapters describing the process model. Furthermore, I have integrated the comparison of different process models of the co-author into the publication. All the illustrations in this paper were created by me as a basis for current and further research work.		
3	Information security management in German local government **(Section 6)**	**(Moses et al., 2022b)** Moses, F., Sandkuhl, K., Kemmerich, T., 2022b. Information security management in German local government. Presented at the 17th Conference on Computer Science and Intelligence Systems, pp. 183–189. https://doi.org/10.15439/2022F162	**18,96% acceptance rate**
Contribution	This paper is based on various case studies and their analyses. The core of the publication is the literature research, which I was responsible for conducting and preparing for publication. The case studies were analysed using a coding scheme developed by me and the results summarised in the paper. The results were critically discussed with the co-authors. I took the results of this discussion into account in the article.		

#	Title	Reference / Publishing body	Acceptance Rate / Ranking
4	Mit CISIS12 ein ISMS aufbauen **(Section 7)**	**(Moses and Sandkuhl, 2022)** Moses, F., Sandkuhl, K., 2022. Mit CISIS12 ein ISMS aufbauen. DuD Springer 46, 654–659. https://doi.org/10.1007/s11623-022-1677-5	**Jourqual D, Acceptance rate ca. 35%**
Contribution	I also carried out extensive literature research for this publication. At the same time, I supervised an increasing number of field studies as part of the research work, permanently analysing their results and publishing them in this publication. As the main author, I planned, structured and discussed the publication. Sections 1-5 were written by me. Section 6 was refined accordingly after discussion with the co-author and the literature research was re-examined and adapted. This was the first article in which the vision and core idea of the process model was presented. As the author, I am responsible for the proposed model and its anchoring in the literature.		
5	Federal Cybersecurity Architecture and Information Security Management – Adoption and Diffusion of the NIS-2 Requirements **(Section 8)**	**(Moses and Rehbohm, 2023b)** Moses, F., Rehbohm, T., 2023a. Federal Cybersecurity Architecture and Information Security Management - Adoption and Diffusion of the NIS-2 Requirements, in: Auth, G., Pidun, T. (Eds.), GI Edition Proceedings Band 341 6. Fachtagung Rechts- Und Verwaltungsinformatik (RVI 2023). Gesellschaft für Informatik e.V., Bonn.	**ca. 48% acceptance rate**
Contribution	For this publication, I created sections 1-3 and 5-7. Section 6 was supplied by the co-author, and I incorporated it into the publication. I carried out the literature research in its entirety. I also created the graphics used in the paper. I also integrated the requirements of the NIS2 guideline supplied by the co-author into section 6. The implementation option using the procedure model developed by me is described accordingly.		
6	Föderale Cybersicherheitsarchitektur und Informationssicherheits-management im Kontext der NIS-2-Richtlinie	**(Moses and Rehbohm, 2023a)** Moses, F., Rehbohm, T., 2023b. Föderale Cybersicherheitsarchitektur und Informationssicherheitsmanagement im Kontext der NIS-2-Richtlinie. Datenschutz Datensicherheit DuD 47, 648–655. https://doi.org/10.1007/s11623-023-1837-2	**Jourqual D, Acceptance rate ca. 35%**
Contribution	I planned and wrote most of the article in consultation with the co-author. Sections 1 and 2 were written by me. Section 3, supplied by the co-author, was incorporated into the publication by me. All graphics used were created by me. The requirements of the NIS2 directive, which have changed over time, were reviewed by me and discussed again in this publication and integrated into the solution approach.		

#	Title	Reference / Publishing body	Acceptance Rate / Ranking
7	ISMS in Small Public Sector Organisations: Requirements and Design of a Procedural Approach	**(Moses and Sandkuhl, 2023)** Moses, F., Sandkuhl, K., 2023. ISMS in small public sector organisations: requirements and design of a procedural approach, in: Morichetta, A., Buchmann, R.A., Sandkuhl, K., Seigerroth, U., Kirikova, M., Møller, C., Forbrig, P., Gutschmidt, A., Ghiran, A.-M., Marcelletti, A., Härer, F., Re, B., Johansson, B. (Eds.), Joint Proceedings of the BIR 2023 Workshops and Doctoral Consortium, CEUR Workshop Proceedings. Presented at the BIR 2023 Workshops and Doctoral Consortium, CEUR, Ascoli Piceno, Italy, pp. 1–10.	**38% acceptance rate**
Contribution	I initiated, designed and conducted the literature research on which the article is based. I also planned the entire scope of the research and co-supervised the research. I discussed the detailed literature analysis and integrated it into a framework with 60 requirements, which served as the basis for further research. Corresponding requirements for further research were derived from this and thus laid the foundation for the process model. The co-author supported me in the application of the DSR approach and thus further structured the research work. All graphics used were created by me.		
8	Entwicklung eines modularen ISMS und DSM	**(Moses and Rehbohm, 2023c)** Moses, F., Rehbohm, T., 2023c. Entwicklung eines modularen ISMS und DSMS. Datenschutz Datensicherheit DuD 47, 721–726. https://doi.org/10.1007/s11623-023-1850-5	**Jourqual D, Acceptance rate ca. 35%**
Contribution	The co-author and I shared responsibility for the article and structured the paper together. I wrote paragraphs 1-3 and 5. I also conducted the literature research for these paragraphs. This also resulted in the overview of the similarities between ISO27701 and the EU-GDPR presented in section 1. This is followed by a description of the integration of data protection into an ISMS. The results were discussed with the co-author, and I incorporated the optimisations resulting from the discussion into the paper. The graphics used were created by me and adapted to the requirements of the publications.		

#	Title	Reference / Publishing body	Acceptance Rate / Ranking
9	CISIS12-Modell: In zwölf einfachen Schritten zum ISMS	**(Moses and Rehbohm, 2023d)** Moses, F., Rehbohm, T., 2023d. CISIS12 für kleine und mittelständische Organisationen IN ZWÖLF SCHRITTEN ZUM RECHTSKONFORMEN ISMS. IT-Sicherheit 14–19.	**ca. 40% acceptance rate**
Contribution	As part of the research process, both the process model and the supporting software were regularly optimised and further developed. Against this background, I planned, structured and discussed this article in its entirety in order to publish the new findings. The co-author intensively reviewed the article as well as the process model and software. The subsequent discussion provided valuable insights, which I incorporated into the article. The process and architecture concept presented in the article is a revised version and extension of my process model presented in previous publications.		
10	Information Security Management in Small Public Sector Organisations: Requirements and Design of a Procedural Approach **(Section 9)**	**(Moses and Sandkuhl, 2024a)** Moses, F., Sandkuhl, K., 2024. Information Security Management in Small Public Sector Organizations: Requirements and Design of a Procedural Approach. Complex Systems Informatics and Modeling Quarterly 54–68. https://doi.org/10.7250/csimq.2023-37.03	**32% acceptance rate**
Contribution	I initiated and conceptualized the article in consultation with the co-author. I conducted the literature analysis in its entirety and was responsible for sections 1-6. The content is based on the extensive literature analysis, the progress of the development of the procedure model and numerous intensive research discussions and investigations with participants in the field study. I was in charge of supervising the field studies (2019-2024), analysing and summarising the research results.		
11	Information Security in small Public Sector Organisations: Design and Evaluation of a procedural Approach **(Section 10)**	(**Moses and Sandkuhl, 2024b)** Moses, F. and Sandkuhl, K. Information Security in small Public Sector Organisations: Design and Evaluation of procedural Approach, in Proceedings of Ninth International Congress on Information and Communication Technology, X.-S. Yan, R. S. Sherratt, N. Dey, and A. Joshi, Eds., London: Springer, 2024.	**20,2% acceptance rate**
Contribution	For this article, I reviewed the literature, planned and structured the article. In essence, I developed an evaluation scheme as part of the article. With its help, the artefacts developed were then examined using a 5-stage evaluation procedure to establish the proof of applicability, usefulness, comprehensiveness and correctness. During the discussion, the co-author made valuable contributions with regard to the evaluation strategy, which I incorporated into the paper.		

#	Title	Reference / Publishing body	Acceptance Rate / Ranking
12	CISO as a Driver of an ISMS in Public Sector Administrations **(Section 11)**	**(Moses and Sandkuhl, 2024c)** Moses, F., Sandkuhl, K. CISO as a Driver of an ISMS in Public Sector Administrations, in *Human Centred Intelligent Systems. Proceedings of KES-HCIS 2024 Conference*, A. Zimmermann, R. Schmidt, L. C. Jain, and R. J. Howlett, Eds., Springer, 2024.	**27% acceptance rate**
Contribution	I researched the literature for this article. As the author, I conceptualised and structured the paper in its entirety. Essentially, this paper is both a report on my experiences and a summary of the difficulties encountered during the research period. The article was written by me and the content was discussed with the co-author. Comments derived from the discussion with the co-author were incorporated into the paper by me.		
13	Risikomanagement in der öffentlichen Verwaltung	**(Moses, 2024)** Moses, F. Risikomanagement: Fundament einer GRC-Gesamt-Architektur, DuD Springer, pp. 442–449, Jul. 2024. https://doi: 10.1007/s11623-024-1954-6.	**Jourqual D, Acceptance rate ca. 35%**
Contribution	I conducted the entire literature research for this article. The publication was initiated, planned and structured by me. In particular, with this article I have highlighted a missing component of the research work. The topic of risk management in particular is one of the key success factors of the process model developed as part of the research work. Sections 1-7 were created by me, including all the graphics used. At the same time, the results of numerous research discussions were taken into account in this article.		

14 Literature References

Abts, D., Mülder, W., 2017. Informationssicherheit, in: Grundkurs Wirtschaftsinformatik. Springer Fachmedien Wiesbaden, Wiesbaden, pp. 601–635. https://doi.org/10.1007/978-3-658-16379-2_17

Ahmad, A., Maynard, S.B., Park, S., 2014. Information security strategies: towards an organizational multi-strategy perspective. J Intell Manuf 25, 357–370. https://doi.org/10.1007/s10845-012-0683-0

Ahmad, S.U., Kashyap, S., Shetty, S.D., Sood, N., 2022. Cybersecurity During COVID-19, in: Joshi, A., Mahmud, M., Ragel, R.G., Thakur, N.V. (Eds.), Information and Communication Technology for Competitive Strategies (ICTCS 2020), Lecture Notes in Networks and Systems. Springer Singapore, Singapore, pp. 1045–1056. https://doi.org/10.1007/978-981-16-0739-4_96

Al Yami, M., Ajmal, M.M., Balasubramanian, S., 2021. Does size matter? The effects of public sector organizational size' on knowledge management processes and operational efficiency. VINE Journal of Information and Knowledge Management Systems 52, 670–700. https://doi.org/10.1108/VJIKMS-07-2020-0123

Alagarsamy, S., Selvaraj, K., Govindaraj, V., Kumar, A.A., HariShankar, S., Narasimman, G.L., 2021. Automated Data analytics approach for examining the background economy of Cybercrime, in: 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA). Presented at the 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), IEEE, Coimbatore, India, pp. 332–336. https://doi.org/10.1109/ICIRCA51532.2021.9544845

Alahmari, A., Duncan, B., 2020. Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence, in: 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). Presented at the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), IEEE, Dublin, Ireland, pp. 1–5. https://doi.org/10.1109/CyberSA49311.2020.9139638

Albayrak, C.A., Gadatsch, A., 2017. Digitalisierung für kleine und mittlere Unternehmen (KMU): Anforderungen an das IT-Management, in: Knoll, M., Strahringer, S. (Eds.), IT-GRC-Management - Governance, Risk und Compliance: Grundlagen und Anwendungen, Edition HMD. Springer Vieweg, Wiesbaden [Heidelberg]. https://doi.org/10.1007/978-3-658-20059-6

Alguliyev, R., Imamverdiyev, Y., Sukhostat, L., 2018. Cyber-physical systems and their security issues. Computers in Industry 100, 212–223. https://doi.org/10.1016/j.compind.2018.04.017

Alharbe, M.A., 2021. Measuring the Influence of Methods to Raise the E-Awareness of Cybersecurity for Medina Region Employees, in: Saeed, F., Al-Hadhrami, T., Mohammed, F., Mohammed, E. (Eds.), Advances on Smart and Soft Computing, Advances in Intelligent Systems and Computing. Springer Singapore, Singapore, pp. 403–410. https://doi.org/10.1007/978-981-15-6048-4_35

Alhashim, S.S., Rahman, M.M.H., 2021. Cybersecurity Threats in Line with Awareness in Saudi Arabia, in: 2021 International Conference on Information Technology (ICIT). Presented at the 2021 International Conference on Information Technology (ICIT), IEEE, Amman, Jordan, pp. 314–319. https://doi.org/10.1109/ICIT52682.2021.9491711

Alkhudhayr, F., Alfarraj, S., Aljameeli, B., Elkhdiri, S., 2019. Information Security:A Review of Information Security Issues and Techniques, in: 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS). Presented at the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), pp. 1–6. https://doi.org/10.1109/CAIS.2019.8769504

Allen, J.H., 2015. Structuring the Chief Information Security Officer Organization.

Alm, R., Wißotzki, M., 2013. TOGAF Adaption for Small and Medium Enterprises, in: Abramowicz, W. (Ed.), Business Information Systems Workshops, Lecture Notes in Business Information Processing. Springer, Berlin, Heidelberg, pp. 112–123. https://doi.org/10.1007/978-3-642-41687-3_12

Al-Mohannadi, H., Awan, I., Al Hamar, J., Al Hamar, Y., Shah, M., Musa, A., 2018. Understanding Awareness of Cyber Security Threat among IT Employees, in: 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). Presented at the 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), IEEE, Barcelona, pp. 188–192. https://doi.org/10.1109/W-FiCloud.2018.00036

Alyami, A., Sammon, D., Neville, K., Mahony, C., 2022. The Critical Success Factors for Security Education, Training and Awareness (SETA) Programmes, in: 2022 Cyber Research Conference - Ireland (Cyber-RCI). Presented at the 2022 Cyber Research Conference - Ireland (Cyber-RCI), IEEE, Galway, Ireland, pp. 1–12. https://doi.org/10.1109/Cyber-RCI55324.2022.10032674

Aman, W., Shukaili, J.A., 2021. A Classification of Essential Factors for the Development and Implementation of Cyber Security Strategy in Public Sector Organizations. IJACSA 12. https://doi.org/10.14569/IJACSA.2021.0120820

Andreasson, A., Artman, H., Brynielsson, J., Franke, U., 2021. A Census of Swedish Public Sector Employee Communication on Cybersecurity during the COVID-19 Pandemic, in: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). Presented at the 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), IEEE, Dublin, Ireland, pp. 1–8. https://doi.org/10.1109/CyberSA52016.2021.9478241

Andreasson, K.J. (Ed.), 2012. Cybersecurity: public sector threats and responses, Public administration and public policy. CRC Press, Boca Raton, FL.

Arbanas, K., Žajdela Hrustek, N., 2019. Key Success Factors of Information Systems Security. Journal of Information and Organizational Sciences 43, 131–144. https://doi.org/10.31341/jios.43.2.1

Archer, L.B., 1984. Systematic method for designers 57–82.

Arreola González, A., Becker, K., Cheng, C.-H., Döricht, V., Duchon, M., Fehling, M., Grolman, H. von, Hallensleben, S., Hopf, S., Ivandic, N., Klein, C., Läßle, E., Lindner, J., Neuburger, R., Prehofer, C., Schätz, B., Scholdan, R., Schorp, K., Sedlmeir, J., Vittorias, I., Walckhoff, S., Wenger, M., Zoitl, A., 2016. Digitale Transformation - Wie Informations- und Kommunikationstechnologie etablierte Branchen grundlegend verändert. Ludwig-Maximilians-Universität München, München.

Ashenden, D., Sasse, A., 2013. CISOs and organisational culture: Their own worst enemy? Computers & Security 39, 396–405. https://doi.org/10.1016/j.cose.2013.09.004

Atanassov, V., 2019. Implementation Hierarchy and CIO Organization in Bulgaria's Public Administration.

Auth, G., Von Der Heyde, M., 2022. Die Rolle des Chief Digital Officers für die digitale

Transformation von Hochschulen. HMD 59, 867–880. https://doi.org/10.1365/s40702-022-00869-6

Awan, J.H., 2017. Security strategies to overcome cyber measures, factors and barriers. Engineering Science and Technology International Research Journal Vol.1, No. 1.

Bada, M., Sasse, A.M., Nurse, J.R.C., 2014. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?

BAFIN, 2017. Rundschreiben 10/2017 (BAFIN) [WWW Document]. BaFin. URL https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.html (accessed 12.7.23).

Balta, D., Krcmar, H., Technische Universität München, Lehrstuhl für Wirtschaftsinformatik, Deutschland, 2020. Was sind Herausforderungen proaktiver Verwaltungsleistungen in Deutschland?, in: WI2020 Zentrale Tracks. GITO Verlag, pp. 554–559. https://doi.org/10.30844/wi_2020_e4-kuhn

Bär, C., Grädler, T., Mayr, R. (Eds.), 2018. Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht. Springer Gabler, Berlin.

Bartling, B., Fischbacher, U., 2012. Shifting the Blame: On Delegation and Responsibility. The Review of Economic Studies 79, 67–87. https://doi.org/10.1093/restud/rdr023

Bartsch, M., Frey, S., 2017. Cyberstrategien für Unternehmen und Behörden. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-16139-2

Bauer, A., Günzel, H., 2013. Data-Warehouse-Systeme: Architektur, Entwicklung, Anwendung. dpunkt.verlag.

Bea, F.X., Göbel, E., 2019. Organisation: Theorie und Gestaltung, 5., vollständig überarbeitete Auflage. ed, utb Betriebswirtschaftslehre. UVK Verlag, München.

Becker, F.G., Fallgatter, M.J., 2005. Strategische Unternehmungsführung: eine Einführung - mit Aufgaben und Lösungen. Erich Schmidt, Berlin.

Becker, J., Delfmann, P., Knackstedt, R., Kuropka, D., 2002. Konfigurative Referenzmodellierung, in: Becker, J., Knackstedt, R. (Eds.), Wissensmanagement mit Referenzmodellen: Konzepte für die Anwendungssystem- und Organisationsgestaltung. Physica-Verlag HD, Heidelberg, pp. 25–144. https://doi.org/10.1007/978-3-642-52449-3_2

Becker, J., Holten, R., Knackstedt, R., Niehaves, B., 2003. Forschungsmethodische Positionierung in der Wirtschaftsinformatik: Epistemologische, ontologische und linguistische Leitfragen.

Becker, J., Niehaves, B., 2007. Epistemological perspectives on IS research: a framework for analysing and systematizing epistemological assumptions. Information Systems Journal 17, 197–214. https://doi.org/10.1111/j.1365-2575.2007.00234.x

Benbasat, I., Goldstein, D.K., Mead, M., 1987. The Case Research Strategy in Studies of Information Systems. MIS Quarterly 11, 369–386. https://doi.org/10.2307/248684

Benbasat, I., Zmud, R.W., 2003. The Identity Crisis within the Is Discipline: Defining and Communicating the Discipline's Core Properties. MIS Quarterly 27, 183–194. https://doi.org/10.2307/30036527

Bendiek, A., Schallbruch, M., 2019. Europas dritter Weg im Cyberraum: der Beitrag der neuen Cybersicherheitsverordnung. SWP-Aktuell. https://doi.org/10.18449/2019A60

Benner-Wickner, M., Kneuper, R., Schlömer, I., 2020. Leitfaden für die Nutzung von Design Science Research in Abschlussarbeiten.

Benson, V., McAlaney, J., Frumkin, L.A., 2019. Emerging Threats for the Human Element and

Countermeasures in Current Cyber Security Landscape. Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications 1264–1269. https://doi.org/10.4018/978-1-5225-8897-9.ch062

Bernhardt, W., 2018. Digitalisierung im Spannungsfeld der gesetzlichen Kompetenzträger, in: Bär, C., Grädler, T., Mayr, R. (Eds.), Digitalisierung Im Spannungsfeld von Politik, Wirtschaft, Wissenschaft Und Recht. Springer Gabler, Berlin.

Berthel, J., Becker, F.G., 2003. Personal-Management: Grundzüge für Konzeptionen betrieblicher Personalarbeit, 7., überarb. und erw. Aufl. ed. Schäffer-Poeschel, Stuttgart.

Bertschek, I., Janßen, R., n.d. Cybersicherheit und Innovationen: Ergebnisse einer repräsentativen Umfrage.

Birk, D., 2021. Managed Security Services: Hilfe oder Herausforderung für die Informationssicherheit?: Eine kritische Betrachtung der Vor- und Nachteile. Datenschutz Datensich 45, 676–679. https://doi.org/10.1007/s11623-021-1513-3

Bogumil, J., Jann, W., 2020. Verwaltung und Verwaltungswissenschaft in Deutschland: Eine Einführung. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-28408-4

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

Boos, P., Geckil, C., Muster, J., 2023. Schneller, weiter, besser? Legitimationssicherung der digitalisierten Verwaltung, in: Wagener, A., Stark, C. (Eds.), Die Digitalisierung des Politischen: Theoretische und praktische Herausforderungen für die Demokratie, Sozialwissenschaften und Berufspraxis. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-38268-1

Borchardt, A., Göthlich, S.E., 2009. Erkenntnisgewinnung durch Fallstudien, in: Albers, S., Klapper, D., Konradt, U., Walter, A., Wolf, J. (Eds.), Methodik der empirischen Forschung. Gabler Verlag, Wiesbaden. https://doi.org/10.1007/978-3-322-96406-9

Bortz, J., Döring, N., 2006. Forschungsmethoden und Evaluation: für Human- und Sozialwissenschaftler ; mit 87 Tabellen, 4., überarb. Aufl. ed, Springer-Lehrbuch Bachelor, Master. Springer-Medizin-Verl, Heidelberg.

Borum, R., Felker, J., Kern, S., Dennesen, K., Feyes, T., 2015. Strategic cyber intelligence. Information & Computer Security 23, 317–332. https://doi.org/10.1108/ICS-09-2014-0064

Bostelmann, L., 2021. Cybersicherheit bei der Umsetzung des Onlinezugangsgesetzes - Digitalisierung ja, aber (rechts)sicher!, in: Seckelmann, M., Brunzel, M. (Eds.), Handbuch Onlinezugangsgesetz: Potenziale - Synergien - Herausforderungen. Springer, Berlin.

Bouzoubaa, K., Taher, Y., Nsiri, B., 2021. Predicting DOS-DDOS Attacks: Review and Evaluation Study of Feature Selection Methods based on Wrapper Process. IJACSA 12. https://doi.org/10.14569/IJACSA.2021.0120517

Braun, M., 2021. Impulse einer präventiven Arbeitsgestaltung zur Digitalisierung der öffentlichen Verwaltung. Zbl Arbeitsmed 71, 75–80. https://doi.org/10.1007/s40664-020-00408-4

Brunzel, M., 2021. Lebensqualität, Gemeinwohl und Wertschöpfung – zur Renaissance der Kommune in Zeiten fortschreitender Digitalisierung und Vernetzung, in: Seckelmann, M., Brunzel, M. (Eds.), Handbuch Onlinezugangsgesetz: Potenziale - Synergien - Herausforderungen. Springer, Berlin.

BSI (Ed.), 2023. IT-Grundschutz-Kompendium, Unternehmen und Wirtschaft.

Bundesanzeiger-Verl, Köln.

BSI, 2022. Die Lage der IT-Sicherheit in Deutschland 2022. BSI, Bonn.

BSI, 2021. Die Lage der IT-Sicherheit in Deutschland 2021. BSI, Bonn.

BSI, 2020. Die Lage der IT-Sicherheit in Deutschland 2020. BSI, Bonn.

BSI (Ed.), 2017. Leitfaden zur Basis-Absicherung nach IT-Grundschutz.

BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS) [WWW Document], 2024. . Bundesamt für Sicherheit in der Informationstechnik. URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.html?nn=128578 (accessed 2.26.22).

BSI-Standard 200-2: IT-Grundschutz Methodik [WWW Document], 2024. . Bundesamt für Sicherheit in der Informationstechnik. URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html;jsessionid=FB94937E9D1A22B192408C5C086549F5.internet082?nn=132646 (accessed 10.30.21).

BSI-Standard 200-3: Risikomanagement [WWW Document], 2024. . Bundesamt für Sicherheit in der Informationstechnik. URL https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.html?nn=128620 (accessed 2.26.22).

BSI-Standard 200-4: Business Continuity Management [WWW Document], 2024. . Bundesamt für Sicherheit in der Informationstechnik. URL https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management.html;jsessionid=2F9B51362B3B321EEDF951E9AFF7A592.internet081?nn=531576 (accessed 10.30.21).

BSI-Standards [WWW Document], 2024. . Bundesamt für Sicherheit in der Informationstechnik. URL https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards.html?nn=128646 (accessed 2.4.24).

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

Bundesverfassungsgericht, 1982. Entscheidungen der amtlichen Sammlung - 2 BvR 1187/80.

Calder, A., 2018. EU GDPR: A Pocket Guide, Second Edition. IT Governance Ltd.

Chainey, S.P., Alonso Berbotto, A., 2022. A structured methodical process for populating a crime script of organized crime activity using OSINT. Trends Organ Crim 25, 272–300. https://doi.org/10.1007/s12117-021-09428-9

Chodakowska, A., KAŃDUŁA, S., PRZYBYLSKA, J., 2022. Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done. Lex Localis - Journal of Local Self-Government Vol. 20, No. 1.

Choejey, P., Murray, D., Che Fung, C., 2016. Exploring Critical Success Factors for Cybersecurity in Bhutan's Government Organizations, in: Computer Science & Information Technology (CS & IT). Presented at the Eighth International Conference on Networks &

Communications, Academy & Industry Research Collaboration Center (AIRCC), pp. 49–61. https://doi.org/10.5121/csit.2016.61505

Choi, I., Lee, J., Kwon, T., Kim, K., Choi, Y., Song, J., 2021. An Easy-to-use Framework to Build and Operate AI-based Intrusion Detection for In-situ Monitoring, in: 2021 16th Asia Joint Conference on Information Security (AsiaJCIS). Presented at the 2021 16th Asia Joint Conference on Information Security (AsiaJCIS), IEEE, Seoul, Korea, Republic of, pp. 1–8. https://doi.org/10.1109/AsiaJCIS53848.2021.00011

Ciekanowski, M., Zurawski, S., Ciekanowski, Z., Pauliuchuk, Y., Czech, A., 2024. Chief Information Security Officer: A Vital Component of Organizational Information Security Management. ERSJ XXVII, 35–46. https://doi.org/10.35808/ersj/3370

Clemith, H.J., Sicker, D.C., 2014. Maturity and Process Capability Models and Their Use in Measuring Resilience in Critical Infrastructure Protection Sectors. IJSITA 5, 44–63. https://doi.org/10.4018/ijsita.2014040104

Cleven, A., Gubler, P., Hüner, K.M., 2009. Design alternatives for the evaluation of design science research artifacts, in: Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, DESRIST '09. Association for Computing Machinery, New York, NY, USA, pp. 1–8.

CMMI Institute - Home [WWW Document], n.d. URL https://cmmiinstitute.com/ (accessed 10.31.21).

Comelli, G., Rosenstiel, L. von, 2011. Führung durch Motivation: Mitarbeiter für Unternehmensziele gewinnen. Vahlen.

Cooke, P., 2017. 'Digital tech' and the public sector: what new role after public funding? European Planning Studies 25, 739–754. https://doi.org/10.1080/09654313.2017.1282067

Coppolino, L., D'Antonio, S., Mazzeo, G., Romano, L., Sgaglione, L., 2018. How to Protect Public Administration from Cybersecurity Threats: The COMPACT Project, in: 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA). Presented at the 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), IEEE, Krakow, pp. 573–578. https://doi.org/10.1109/WAINA.2018.00147

Çubuk, E.B.S., Zeren, H.E., Demirdöven, B., 2022. The Role of Data Governance in Cybersecurity for E-Municipal Services: Implications From the Case of Turkey, in: Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications. IGI Global, pp. 410–425. https://doi.org/10.4018/978-1-6684-5284-4.ch020

Da Silva, J., Jensen, R.B., 2022. "Cyber security is a dark art": The CISO as Soothsayer. Proc. ACM Hum.-Comput. Interact. 6, 1–31. https://doi.org/10.1145/3555090

De Abrew, K.M.N., Wickramarachchi, R., 2021. Organizational Factors Affecting the ISMS Effectiveness in Sri Lankan IT Organizations: A Systematic Review.

Destatis [WWW Document], 2024. . Statistisches Bundesamt. URL https://www.destatis.de/DE/Themen/Laender-Regionen/Regionales/Gemeindeverzeichnis/Administrativ/08-gemeinden-einwohner-groessen.html (accessed 2.3.24).

Dibbern, J., Goles, T., Hirschheim, R., Jayatilaka, B., 2004. Information systems outsourcing: a survey and analysis of the literature. SIGMIS Database 35, 6–102. https://doi.org/10.1145/1035233.1035236

Diethelm, I., Dörge, C., Hildebrandt, C., Gesellschaft für Informatik (Eds.), 2010. Didaktik der Informatik - Möglichkeiten empirischer Forschungsmethoden und Perspektiven der

Fachdidaktik: 6. Workshop der GI-Fachgruppe “Didaktik der Informatik”, 16. - 17. September 2010 in Oldenburg, GI-Edition lecture notes in informatics P, Proceedings. Presented at the Workshop Didaktik der Informatik, Ges. für Informatik (GI), Bonn.

DiMaggio, P.J., Powell, W.W., 1983. The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. American Sociological Review 48, 147–160. https://doi.org/10.2307/2095101

DIN ISO/IEC 27000, 2016. . DIN.

DIN ISO/IEC 27001, 2018. . DIN.

Dreißigacker, A., Skarczinski, B. von, Wollinger, G.R., 2021. Cyberangriffe gegen Unternehmen in Deutschland: Ergebnisse einer Folgebefragung 2020, Forschungsbericht / KFN, Kriminologisches Forschungsinstitut Niedersachsen e.V. Kriminologisches Forschungsinstitut Niedersachsen e.V. (KFN), Hannover.

Dreyling, R., Jackson, E., Pappel, I., 2021. Cyber Security Risk Analysis for a Virtual Assistant G2C Digital Service Using FAIR Model, in: 2021 Eighth International Conference on eDemocracy & eGovernment (ICEDEG). Presented at the 2021 Eighth International Conference on eDemocracy & eGovernment (ICEDEG), IEEE, Quito, Ecuador, pp. 33–40. https://doi.org/10.1109/ICEDEG52154.2021.9530938

Drmola, J., Kasl, F., Loutocký, P., Mareš, M., Pitner, T., Vostoupal, J., 2021. The Matter of Cybersecurity Expert Workforce Scarcity in the Czech Republic and Its Alleviation Through the Proposed Qualifications Framework, in: The 16th International Conference on Availability, Reliability and Security. Presented at the ARES 2021: The 16th International Conference on Availability, Reliability and Security, ACM, Vienna Austria, pp. 1–6. https://doi.org/10.1145/3465481.3469186

DSGVO: EU-Datenschutz-Grundverordnung; 2021; aktuelle Gesetze, 7. Auflage, Rechtsstand: September 2021. ed, 2021. . Harwardt, Erscheinungsort nicht ermittelbar.

Dürig, M., Fischer, M., 2018. Cybersicherheit in Kritischen Infrastrukturen: Europäische und deutsche Regulierung — ein Überblick. Datenschutz und Datensicherheit - DuD 42, 209–213. https://doi.org/10.1007/s11623-018-0909-1

Ebel, N., 2021. Basiswissen ITIL 4: Grundlagen und Know-how für das IT Service Management und die ITIL-4-Foundation-Prüfung. dpunkt.verlag.

Eckhardt, P., Kotovskaia, A., 2023. The EU’s cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. Int. Cybersecur. Law Rev. 4, 147–164. https://doi.org/10.1365/s43439-023-00084-z

Eekels, J., Roozenburg, N.F.M., 1991. A methodological comparison of the structures of scientific research and engineering design: their similarities and differences. Design Studies 12, 197–203. https://doi.org/10.1016/0142-694X(91)90031-Q

EGovG - Gesetz zur Förderung der elektronischen Verwaltung, n.d.

Eisenhardt, K.M., 1989. Building Theories from Case Study Research. AMR 14, 532–550. https://doi.org/10.5465/amr.1989.4308385

Engels, B., 2021. Cybersicherheit: 52,5 Mrd. Euro Schaden durch Angriffe im Homeoffice.

Engländer, J., Kaminski, L., Schuba, M., 2022. Informationssicherheitsmanagement, in: Schuh, G., Zeller, V., Stich, V. (Eds.), Digitalisierungs- und Informationsmanagement: Handbuch Produktion und Management 9. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-63758-6

Europäisches Parlaments und Rat, 2023. Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie), 2022/2555.

Farrand, B., Carrapico, H., 2022. Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity. European Security 31, 435–453. https://doi.org/10.1080/09662839.2022.2102896

Fedele, A., Roner, C., 2022. Dangerous Games: A Literature Review on Cybersecurity Investments. Journal of Economic Surveys 36, 157–187.

Fettke, P., 2006. State-of-the-Art des State-of-the-Art: Eine Untersuchung der Forschungsmethode „Review" innerhalb der Wirtschaftsinformatik. Wirtsch. Inform. 48, 257–266. https://doi.org/10.1007/s11576-006-0057-3

Fettke, P., Loos, P., 2004. Referenzmodellierungsforschung. Wirtschaftsinf 46, 331–340. https://doi.org/10.1007/BF03250947

Fettke, P., Loos, P., 2002. Der Referenzmodellkatalog als Instrument des Wissensmanagements: Methodik und Anwendung, in: Becker, J., Knackstedt, R. (Eds.), Wissensmanagement mit Referenzmodellen: Konzepte für die Anwendungssystem- und Organisationsgestaltung. Physica-Verlag HD, Heidelberg, pp. 3–24. https://doi.org/10.1007/978-3-642-52449-3_1

Fischer, C., 2010. Auf dem Weg zu Kriterien zur Auswahl einer geeigneten Evaluationsmethode für Artefakte der gestaltungsorientierten Wirtschaftsinformatik. Gesellschaft für Informatik e.V.

FIT, 2024. Digitale Transformation [WWW Document]. URL https://www.wi.fit.fraunhofer.de/de/geschaeftsfelder.html (accessed 2.16.24).

Fitzgerald, T., 2007. Clarifying the Roles of Information Security: 13 Questions the CEO, CIO, and CISO Must Ask Each Other. Information Systems Security 16, 257–263. https://doi.org/10.1080/10658980701746577

Forrester, J., Lopez, M.L., Valentina, M.D., 2022. Marketing a cybersecurity Awareness Solution in LPA Contexts, in: Andriessen, J., Schaberreiter, T., Papanikolaou, A., Röning, J. (Eds.), Cybersecurity Awareness, Advances in Information Security. Springer International Publishing, Cham, pp. 161–181. https://doi.org/10.1007/978-3-031-04227-0_7

Frank, U., Lange, C., 1999. Aktionsforschung in der WI - Einsatzpotentiale und Einsatzprobleme, in: Schütte, R., Siedentopf, J., Zelewski, S. (Eds.), Wirtschaftsinformatik Und Wissenschaftstheorie - Grundpositionen Und Theoriekerne. Arbeitsbericht Nr. 46,. Essen.

Frankenstein, R., 2023. BSI IT-Grundschutz – Arbeitswerkzeug für ganzheitliche Informationssicherheit. Datenschutz Datensich 47, 410–415. https://doi.org/10.1007/s11623-023-1788-7

Freiling, F., Grimm, R., Großpietsch, K.-E., Keller, H.B., Mottok, J., Münch, I., Rannenberg, K., Saglietti, F., 2014. Technische Sicherheit und Informationssicherheit: Unterschiede und Gemeinsamkeiten. Informatik Spektrum 37, 14–24. https://doi.org/10.1007/s00287-013-0748-2

Fujs, D., Bernik, I., 2024. Analyzing Cybersecurity Strategies of the European Union: Challenges and Opportunities for Public Administration.

Garba, A.A., Siraj, M.M., Othman, S.H., 2020. An Explanatory Review on Cybersecurity Capability Maturity Models. Adv. sci. technol. eng. syst. j. 5, 762–769. https://doi.org/10.25046/aj050490

Gedris, K., Bowman, K., Neupane, A., Hughes, A.L., Bonsignore, E., West, R.W., Balzotti, J., Hansen, D.L., 2021. Simulating municipal cybersecurity incidents: Recommendations from expert interviews. Presented at the Proceedings of the Annual Hawaii International

Conference on System Sciences, pp. 2036–2045.

Gernot Heller, 2021. Immer mehr Cyberangriffe: IT-Sicherheitsbehörde BSI schlägt Alarm - Professionalität steigt: IT-Sicherheitsbehörde BSI schlägt Alarm - Professionalität steigt. Passauer Neue Presse vom 22.10.2021.

Glaspie, H.W., Karwowski, W., 2018. Human Factors in Information Security Culture: A Literature Review, in: Nicholson, D. (Ed.), Advances in Human Factors in Cybersecurity, Advances in Intelligent Systems and Computing. Springer International Publishing, Cham, pp. 269–280. https://doi.org/10.1007/978-3-319-60585-2_25

Göbel, E., 2021. Neue Institutionenökonomik: Grundlagen, Ansätze und Kritik, utb Wirtschaftswissenschaften. UVK Verlag, München.

Goldenson, D.R., Gibson, D.L., 2003. Demonstrating the Impact and Benefits of CMMI®: An Update and Preliminary Results.

Goodyear, M., Goerdel, H.T., Portillo, S., Williams, L., 2010. Cybersecurity Management In the States: The Emerging Role of Chief Information Security Officers. SSRN Journal. https://doi.org/10.2139/ssrn.2187412

Grigat, M., Jurecz, S., Kirschner, S., Seidel, R., Stepanek, T., 2020. Kosten der IT-Sicherheit: Ein Ausgangspunkt für weitergehende Untersuchungen. BoD – Books on Demand.

Grunwald, K., 2022. Management sozialwirtschaftlicher Organisationen: Eine Einführung, Basiswissen Sozialwirtschaft und Sozialmanagement. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-26340-9

Gulden, H., 2018. Digitalisierung und IT-Sicherheit, in: Bär, C., Grädler, T., Mayr, R. (Eds.), Digitalisierung Im Spannungsfeld von Politik, Wirtschaft, Wissenschaft Und Recht. Springer Gabler, Berlin.

Gusy, C., Kugelmann, D., Würtenberger, T. (Eds.), 2017. Rechtshandbuch Zivile Sicherheit. Springer, Berlin Heidelberg.

Hahn, D., 2020. Risiko-Management in Kommunen: Handlungsorientierter Leitfaden für die kommunale Praxis, Edition Innovative Verwaltung. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-29271-3

Hanschke, I., 2020a. Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten: Eine kompakte Einführung in die Praxis, essentials. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-28699-6

Hanschke, I., 2020b. EAM & CMDB als Erfolgsfaktor für ein wirksames ISMS, in: Hanschke, I. (Ed.), Informationssicherheit und Datenschutz systematisch und nachhaltig gestalten: Eine kompakte Einführung in die Praxis, essentials. Springer Fachmedien, Wiesbaden, pp. 77–81. https://doi.org/10.1007/978-3-658-28699-6_4

Hanschke, I., 2016. Enterprise Architecture Management - einfach und effektiv: ein praktischer Leitfaden für die Einführung von EAM, 2., überarbeitete Auflage. ed. Hanser, München.

Hanschke, I., Schwarz, C., 2019. Informationssicherheit – lean & agil. Wirtsch Inform Manag 11, 216–223. https://doi.org/10.1365/s35764-019-00194-6

Hars, A., 2002. Wissenschaftstheorie für Wirtschaftsinformatiker, in: Multikonferenz Wirtschaftsinformatik 2002. Nürnberg.

Hatcher, W., Meares, W.L., Heslen, J., 2020. The cybersecurity of municipalities in the United States: an exploratory survey of policies and practices. Journal of Cyber Policy 5, 302–325. https://doi.org/10.1080/23738871.2020.1792956

Heerwegh, D., 2006. An Investigation of the Effect of Lotteries on Web Survey Response Rates. Field Methods 18, 205–220. https://doi.org/10.1177/1525822X05285781

Heinemann, D., 2023. EGovG: Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz). De Gruyter.

Heinrich, L.J., Heinzl, A., Riedl, R., 2011. Wirtschaftsinformatik: Einführung und Grundlegung, 4., überarb. und erw. Aufl. ed, Springer-Lehrbuch. Springer, Berlin Heidelberg.

Helbig, N., Ramón Gil-García, J., Ferro, E., 2009. Understanding the complexity of electronic government: Implications from the digital divide literature. Government Information Quarterly, From Implementation to Adoption: Challenges to Successful E-government Diffusion 26, 89–97. https://doi.org/10.1016/j.giq.2008.05.004

Helfert, M., Donnellan, B., Ostrowski, L., 2012. The case for design science utility and quality - Evaluation of design science artifact within the sustainable ICT capability maturity framework. Systems, Signs and Actions: An International Journal on Information Technology, Action, Communication and Workpractices 6, 46–66.

Henning, A., Schulze, A., Meuche, T., Markus, H., 2022. Deutschlandweite Umfrage zum digitalen Reifegrad der öffentlichen Verwaltung auf Kommunalebene : Forschungsbericht. Hochschule für Angewandte Wissenschaften Hof. https://doi.org/10.57944/1051-128

Henseler-Unger, I., Hillebrand, A., 2018. Aktuelle Lage der IT-Sicherheit in KMU: Wie kann man die Umsetzungslücke schließen? Datenschutz Datensich 42, 686–690. https://doi.org/10.1007/s11623-018-1025-y

Hertneck, C., Kneuper, R., 2012. Prozesse verbessern mit CMMI for Services: Ein Praxisleitfaden mit Fallstudien. dpunkt.verlag.

Heuermann, R., Engel, A., von Lucke, J., 2018a. Digitalisierung: Begriff, Ziele und Steuerung, in: Heuermann, R., Tomenendal, M., Bressem, C. (Eds.), Digitalisierung in Bund, Ländern und Gemeinden. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-54098-5

Heuermann, R., Tomenendal, M., Bressem, C. (Eds.), 2018b. Digitalisierung in Bund, Ländern und Gemeinden. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-54098-5

Hevner, A., Chatterjee, S., 2010. Design Science Research in Information Systems, in: Hevner, A., Chatterjee, S. (Eds.), Design Research in Information Systems: Theory and Practice, Integrated Series in Information Systems. Springer US, Boston, MA, pp. 9–22. https://doi.org/10.1007/978-1-4419-5653-8_2

Hevner, A.R., March, S.T., Park, J., Ram, S., 2004. Design Science in Information Systems Research. MIS Quarterly 28, 75–105. https://doi.org/10.2307/25148625

Hof, H.J., 2022. Cybersecurity für den zukunftsfähigen Handel, in: Knoppe, M., Rock, S., Wild, M. (Eds.), Der zukunftsfähige Handel: Neue online und offline Konzepte sowie digitale und KI-basierte Lösungen. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-36218-8

Hohmeister, F., Rückel, D., 2021. Kritische Erfolgsfaktoren für die Auswahl eines IT-Serviceproviders am Beispiel der gesetzlichen Unfallversicherungen. HMD 58, 991–1003. https://doi.org/10.1365/s40702-021-00774-4

Hooper, V., McKissack, J., 2016. The emerging role of the CISO. Business Horizons, CYBERSECURITY IN 2016: PEOPLE, TECHNOLOGY, AND PROCESSES 59, 585–591. https://doi.org/10.1016/j.bushor.2016.07.004

Hopp, H., 2020. Management in der öffentlichen Verwaltung: Organisations- und Personalarbeit in modernen Kommunalverwaltungen. Schäffer-Poeschel.

Hornbostel, L., Tillack, D., Nerger, M., Wittpahl, V., Handschuh, A., Salden, J., 2022. Zukunftsradar Digitale Kommune.

Hron, M., Obwegeser, N., 2022. Why and how is Scrum being adapted in practice: A systematic review. Journal of Systems and Software 183, 111110. https://doi.org/10.1016/j.jss.2021.111110

Hui-Lin, H., Kuei-Min, W., 2014. The critical success factors assessment of ISO 27001 certification in computer organization by test-retest reliability. Afr. J. Bus. Manage. 8, 705–716. https://doi.org/10.5897/AJBM2014.7443

Hunziker, S., Meissner, J.O., 2017. Risikomanagement in 10 Schritten, essentials. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-15840-8

Hwang, Y.-W., Lee, I.-Y., Kim, H., Lee, H., Kim, D., 2022. Current Status and Security Trend of OSINT. Wireless Communications and Mobile Computing 2022, e1290129. https://doi.org/10.1155/2022/1290129

Initiative D21, 2019. D21-Digital-Index 2018/2019 – Jährliches Lagebild zur Digitalen Gesellschaft.

Jäggi, C.J., 2023. Digitalisierung in Wirtschaft und Gesellschaft: Ökonomische, soziale und ökologische Auswirkungen, Fragen und Perspektiven. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-42206-6

Jajodia, S., Albanese, M., 2017. An Integrated Framework for Cyber Situation Awareness, in: Liu, P., Jajodia, S., Wang, C. (Eds.), Theory and Models for Cyber Situation Awareness, Lecture Notes in Computer Science. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-61152-5

Jalali, M.S., Russell, B., Razak, S., Gordon, W.J., 2019. EARS to cyber incidents in health care. Journal of the American Medical Informatics Association 26, 81–90. https://doi.org/10.1093/jamia/ocy148

Jann, W., 2019. Neues Steuerungsmodell, in: Veit, S., Reichard, C., Wewer, G. (Eds.), Handbuch zur Verwaltungsreform. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-21563-7

Johannesson, P., Perjons, E., 2014. An Introduction to Design Science. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-10632-8

Johannsen, W., Goeken, M., 2011. Referenzmodelle für IT-Governance: Methodische Unterstützung der Unternehmens-IT mit COBIT, ITIL & Co. dpunkt.verlag.

Jörgens, F., 2023. The Human Firewall: Wie eine Kultur der Cyber-Sicherheit geschaffen wird, essentials. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-42757-3

Kammerloher, D., 2021. Cybersecurity: Ein sicheres Fundament für den digitalen Staat. Datenschutz Datensich 45, 649–653. https://doi.org/10.1007/s11623-021-1508-0

Kaplan, R.S., 1999. The Balanced Scorecard for Public-Sector Organizations.

Kappers, W.M., Harrell, M.N., 2020. From Degree to Chief Information Security Officer (CISO): A Framework for Consideration.

Karanja, E., 2017. The role of the chief information security officer in the management of IT security. ICS 25, 300–329. https://doi.org/10.1108/ICS-02-2016-0013

Karau, S.J., Williams, K.D., 1993. Social loafing: A meta-analytic review and theoretical

integration. Journal of Personality and Social Psychology 65, 681–706. https://doi.org/10.1037/0022-3514.65.4.681

Katz, R.L., 2009. Skills of an Effective Administrator. Harvard Business Review Press.

Kävrestad, J., Furnell, S., Nohlberg, M., 2021. What Parts of Usable Security Are Most Important to Users?, in: Drevin, L., Miloslavskaya, N., Leung, W.S., von Solms, S. (Eds.), Information Security Education for Cyber Resilience, IFIP Advances in Information and Communication Technology. Springer International Publishing, Cham, pp. 126–139. https://doi.org/10.1007/978-3-030-80865-5_9

KBA, 2014. Internetbasierte Fahrzeugzulassun g (i-Kfz).

Keebler, J.R., Rosen, M.A., Sittig, D.F., Thomas, E., Salas, E., 2022. Human Factors and Ergonomics in Healthcare: Industry Demands and a Path Forward. Hum Factors 64, 250–258. https://doi.org/10.1177/00187208211073623

Kemper, H.G., Finger, R., 2016. Transformation operativer Daten – Konzeptionelle Überlegungen zur Filterung, Harmonisierung, Verdichtung und Anreicherung im Data Warehouse., in: Gluchowski, P., Chamoni, P. (Eds.), Analytische Informationssysteme: Business Intelligence-Technologien und -Anwendungen. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-47763-2

Kersten, H., Reuter, J., Schröder, K.-W., 2013. IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: der Weg zur Zertifizierung, 4., aktualisierte und erw. Aufl. ed, Edition <kes>. Springer Vieweg, Wiesbaden.

Kersting, N., Kuhlmann, S., 2018. Sub-municipal Units in Germany: Municipal and Metropolitan Districts, in: Hlepas, N.-K., Kersting, N., Kuhlmann, S., Swianiewicz, P., Teles, F. (Eds.), Sub-Municipal Governance in Europe, Governance and Public Management. Springer International Publishing, Cham, pp. 93–118. https://doi.org/10.1007/978-3-319-64725-8_5

Kesan, J.P., Zhang, L., 2021. An Empirical Investigation of the Relationship between Local Government Budgets, IT Expenditures, and Cyber Losses. IEEE Trans. Emerg. Topics Comput. 9, 582–596. https://doi.org/10.1109/TETC.2019.2915098

Khansa, L., Kuem, J., Siponen, M., Kim, S.S., 2017. To Cyberloaf or Not to Cyberloaf: The Impact of the Announcement of Formal Organizational Controls. Journal of Management Information Systems 34, 141–176. https://doi.org/10.1080/07421222.2017.1297173

Kipker, D.-K., 2020. Cybersecurity. C.H. Beck, München.

Kipker, D.-K., Barudi, M. (Eds.), 2020. Cybersecurity, 1. Auflage. ed. C.H. Beck, München.

Kitsios, F., Chatzidimitriou, E., Kamariotou, M., 2022. Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. Sustainability 14, 1269. https://doi.org/10.3390/su14031269

Klenk, T., Nullmeier, F., Wewer, G. (Eds.), 2020. Handbuch Digitalisierung in Staat und Verwaltung. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-23668-7

Knodt, Platzer, 2023. Lessons Learned: Koordination im Katastrophenmanagement. Zenodo. https://doi.org/10.5281/ZENODO.7756274

Knoll, M., Strahringer, S. (Eds.), 2017. IT-GRC-Management – Governance, Risk und Compliance, Edition HMD. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-20059-6

Königs, H.-P., 2017. IT-Risikomanagement mit System: Praxisorientiertes Management von

Informationssicherheits-, IT- und Cyber-Risiken. Springer-Verlag.

Koontz, H., O'Donnel, C., 1976. Management: A systems and contingence analysis of managerial functions, 6. Auflage. ed. New York.

Koza, E., 2021. Eine empirische Kontentanalyse zur Ermittlung von praxisorientierten Optimierungsfeldern zur Resilienz-Erhöhung der IT-Systeme im Sinne der ganzheitlichen Betrachtung der Informationssicherheit. Gesellschaft für Informatik, Bonn. https://doi.org/10.18420/informatik2021-070

Krajewski, M. (Ed.), 2015. Services of general interest beyond the single market: external and international law dimensions, Legal issues of services of general interest. T.M.C. Asser Press, The Hague.

Kremer, T., 2018. IT-Sicherheit muss gelebt werden, in: Bär, C., Grädler, T., Mayr, R. (Eds.), Digitalisierung Im Spannungsfeld von Politik, Wirtschaft, Wissenschaft Und Recht. Springer Gabler, Berlin.

Krumm, S., Mertin, I., Dries, C., 2012. Kompetenzmodelle. Hogrefe Verlag GmbH & Company KG.

Kubbe, I., 2020. Experimente und experimentelle Forschungsdesigns, in: Wagemann, C., Goerres, A., Siewert, M.B. (Eds.), Handbuch Methoden der Politikwissenschaft. Springer Fachmedien Wiesbaden, Wiesbaden, pp. 99–126. https://doi.org/10.1007/978-3-658-16936-7

Kuhn, T., 2021. Warum deutsche Kommunen so anfällig für Cyberattacken sind: "Das kannst Du doch keinem erklären." WirtschaftsWoche online 21.10.2021.

Kumar, D.P., 2015. An Analytical study on Mintzberg's Framework: Managerial Roles. International Journal of Research in Management 2.

Kweon, E., Lee, H., Chai, S., Yoo, K., 2021. The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. Inf Syst Front 23, 361–373. https://doi.org/10.1007/s10796-019-09977-z

Lang, T., 2022. Damit der Cyber-Katastrophenfall nicht zum Normalfall wird, müssen wir kritische Infrastrukturen besser schützen – die Lektionen aus dem Fall Bitterfeld. Wirtsch Inform Manag 14, 27–28. https://doi.org/10.1365/s35764-021-00384-1

Lange, C., 2005. Ein Bezugsrahmen zur Beschreibung von Forschungsgegenständen und -methoden in Wirtschaftsinformatik und Information Systems.

Lanz, J., 2017. The Chief Information Security Officer.

Latané, B., Williams, K., Harkins, S., 1979. Many hands make light the work: The causes and consequences of social loafing. Journal of Personality and Social Psychology 37, 822–832. https://doi.org/10.1037/0022-3514.37.6.822

Leeser, D.C., 2020. Digitalisierung in KMU kompakt: Compliance und IT-Security, IT kompakt. Springer Vieweg, Berlin [Heidelberg]. https://doi.org/10.1007/978-3-662-59738-5

Lehto, M., 2020. ECCWS 2020 19th European Conference on Cyber Warfare: Warfare and Security.

Lenhard, T.H., 2020. Datensicherheit: Technische und organisatorische Schutzmaßnahmen gegen Datenverlust und Computerkriminalität. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-29866-1

Lezzi, M., Lazoi, M., Corallo, A., 2018. Cybersecurity for Industry 4.0 in the current literature: A reference framework. Computers in Industry 103, 97–110.

https://doi.org/10.1016/j.compind.2018.09.004

Li, Y., Liu, Q., 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Liedtke, T., 2022. Informationssicherheit: Möglichkeiten und Grenzen. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-63917-7

Lim, V.K.G., Teo, T.S.H., 2005. Prevalence, perceived seriousness, justification and regulation of cyberloafing in Singapore: An exploratory study. Information & Management 42, 1081–1093. https://doi.org/10.1016/j.im.2004.12.002

Lühr, H., 2021. Von der Konferenz „Deutschland online“ zur föderativen IT-Kooperation – Innovation und Digital Leadership im föderalen Mehrebenensystem in Deutschland, in: Seckelmann, M., Brunzel, M. (Eds.), Handbuch Onlinezugangsgesetz: Potenziale - Synergien - Herausforderungen. Springer, Berlin.

Maglaras, L., Drivas, G., Chouliaras, N., Boiten, E., Lambrinoudakis, C., Ioannidis, S., 2020. Cybersecurity in the Era of Digital Transformation: The case of Greece, in: 2020 International Conference on Internet of Things and Intelligent Applications (ITIA). Presented at the 2020 International Conference on Internet of Things and Intelligent Applications (ITIA), IEEE, Zhenjiang, China, pp. 1–5. https://doi.org/10.1109/ITIA50152.2020.9312297

Majid, M.A., Ariffin, K.A.Z., 2021. Model for successful development and implementation of Cyber Security Operations Centre (SOC). PLOS ONE 16, e0260157. https://doi.org/10.1371/journal.pone.0260157

March, S.T., Smith, G.F., 1995. Design and natural science research on information technology. Decision Support Systems 15, 251–266. https://doi.org/10.1016/0167-9236(94)00041-2

Markopoulou, D., Papakonstantinou, V., de Hert, P., 2019. The new EU cybersecurity framework: The NIS Directive, ENISA’s role and the General Data Protection Regulation. Computer Law & Security Review 35, 105336. https://doi.org/10.1016/j.clsr.2019.06.007

Markus, H., Meuche, T., 2022. Auf dem Weg zur digitalen Verwaltung: Ein ganzheitliches Konzept für eine gelingende Digitalisierung in der öffentlichen Verwaltung, Edition Innovative Verwaltung. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-37151-7

Martin, L., Hauret, L., Fuhrer, C., 2022. Digitally transformed home office impacts on job satisfaction, job stress and job productivity. COVID-19 findings. PLoS ONE 17, e0265131. https://doi.org/10.1371/journal.pone.0265131

Martini, M., Fritzsche, S., Kolain, M., 2016. Digitalisierung als Herausforderung und Chance für Staat und Verwaltung - Forschungskonzept des Programmbereichs “Transformation des Staates in Zeiten der Digitalisierung.” FÖV, Speyer.

Mast, C., 2017. Neuerfindung einer Industrie. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-17419-4

Maynard, S.B., Onibere, M., Ahmad, A., 2018. Defining the Strategic Role of the Chief Information Security Officer. PAJAIS 61–86. https://doi.org/10.17705/1pais.10303

Mayring, P., 2015. Qualitative Inhaltsanalyse: Grundlagen und Techniken, 12., überarb. Aufl. ed. Beltz, Weinheim Basel.

Mayring, P., 2004. Qualitative content analysis. A companion to qualitative research, in: Flick, U., Kardoff, E. von, Stein, I. (Eds.), A Companion to Qualitative Research. SAGE, pp. 159–176.

McDermid, J., 1987. The Role of Formal Methods in Software Development. Journal of Information Technology 2, 124–134. https://doi.org/10.1177/026839628700200305

Melzer, A., Heim, Y., Sanders, T., Bullinger-Hoffmann, A.C., 2019. Zur Zukunft des Kompetenzmanagements, in: Bullinger-Hoffmann, A.C. (Ed.), Zukunftstechnologien und Kompetenzbedarfe: Kompetenzentwicklung in der Arbeitswelt 4.0, Kompetenzmanagement in Organisationen. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-54952-0

Mergel, I., 2020. Kompetenzen für die digitale Transformation der Verwaltung. Innov Verwalt 42, 34–36. https://doi.org/10.1007/s35114-020-0209-0

Meuche, T., 2022. Dilemmata und Wege zur Digitalisierung der öffentlichen Verwaltung. Gruppe. Interaktion. Organisation. Zeitschrift für Angewandte Organisationspsychologie (GIO). https://doi.org/10.1007/s11612-021-00612-7

Mierowski, S., 2021. Datenschutz nach DS-GVO und Informationssicherheit gewährleisten: eine kompakte Praxishilfe zur Maßnahmenauswahl: Prozess ZAWAS 4.0, essentials. Springer Vieweg, Wiesbaden.

Mintzberg, H., 1980. The nature of managerial work, 2. Aufl. ed. New York.

Mironeanu, C., Archip, A., Amarandei, C.-M., Craus, M., 2021. Experimental Cyber Attack Detection Framework. Electronics 10, 1682. https://doi.org/10.3390/electronics10141682

Monzelo, P., Nunes, S., 2019. The Role of the Chief Information Security Officer (CISO) in Organizations.

Moser, M., 2018. Bedeutung von Soft Skills in einer sich wandelnden Unternehmenswelt. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-22273-4

Moses, F., 2024. Risikomanagement: Fundament einer GRC-Gesamt-Architektur. DuD Springer 442–449. https://doi.org/10.1007/s11623-024-1954-6

Moses, F., Rehbohm, T., 2023a. Föderale Cybersicherheitsarchitektur und Informationssicherheitsmanagement im Kontext der NIS-2-Richtlinie. DuD Springer 47, 648–655. https://doi.org/10.1007/s11623-023-1837-2

Moses, F., Rehbohm, T., 2023b. Federal Cybersecurity Architecture and Information Security Management - Adoption and Diffusion of the NIS-2 Requirements, in: Auth, G., Pidun, T. (Eds.), GI Edition Proceedings Band 341 6. Fachtagung Rechts- Und Verwaltungsinformatik (RVI 2023). Gesellschaft für Informatik e.V., Bonn.

Moses, F., Rehbohm, T., 2023c. Entwicklung eines modularen ISMS und DSMS. DuD Springer 47, 721–726. https://doi.org/10.1007/s11623-023-1850-5

Moses, F., Rehbohm, T., 2023d. CISIS12 für kleine und mittelständische Organisationen IN ZWÖLF SCHRITTEN ZUM RECHTSKONFORMEN ISMS. IT-Sicherheit 14–19.

Moses, F., Rehbohm, T., 2022a. CISIS12. kes, CISIS12 61–68.

Moses, F., Rehbohm, T., 2022b. CISIS12-Modell: In zwölf einfachen Schritten zum ISMS. Informations-Sicherheit.

Moses, F., Sandkuhl, K., 2024a. Information Security Management in Small Public Sector Organizations: Requirements and Design of a Procedural Approach. Complex Systems Informatics and Modeling Quarterly (CSIMQ) 54–68. https://doi.org/10.7250/csimq.2023-37.03

Moses, F., Sandkuhl, K., 2024b. Information Security in small Public Sector Organisations: Design and Evaluation of procedural Approach, in: Yan, X.-S., Sherratt, R.S., Dey, N., Joshi,

A. (Eds.), Proceedings of Ninth International Congress on Information and Communication Technology. Springer, London.

Moses, F., Sandkuhl, K., 2024c. CISO as a Driver of an ISMS in Public Sector Administrations, in: Zimmermann, A., Schmidt, R., Jain, L.C., Howlett, R.J. (Eds.), Human Centred Intelligent Systems. Proceedings of KES-HCIS 2024 Conference. Springer.

Moses, F., Sandkuhl, K., 2023. ISMS in small public sector organisations: requirements and design of a procedural approach, in: Morichetta, A., Buchmann, R.A., Sandkuhl, K., Seigerroth, U., Kirikova, M., Møller, C., Forbrig, P., Gutschmidt, A., Ghiran, A.-M., Marcelletti, A., Härer, F., Re, B., Johansson, B. (Eds.), Joint Proceedings of the BIR 2023 Workshops and Doctoral Consortium, CEUR Workshop Proceedings. Presented at the BIR 2023 Workshops and Doctoral Consortium, CEUR, Ascoli Piceno, Italy, pp. 1–10.

Moses, F., Sandkuhl, K., 2022. Mit CISIS12 ein ISMS aufbauen. DuD Springer 46, 654–659. https://doi.org/10.1007/s11623-022-1677-5

Moses, F., Sandkuhl, K., Kemmerich, T., 2022a. Empirical Study on the State of Practice of Information Security Management in Local Government, in: Zimmermann, A., Howlett, R.J., Jain, L.C. (Eds.), Human Centred Intelligent Systems, Smart Innovation, Systems and Technologies. Springer Nature, Singapore, pp. 13–25. https://doi.org/10.1007/978-981-19-3455-1_2

Moses, F., Sandkuhl, K., Kemmerich, T., 2022b. Information security management in German local government. Presented at the 17th Conference on Computer Science and Intelligence Systems, pp. 183–189. https://doi.org/10.15439/2022F162

Müller, L.-S., 2018. Digitale Verwaltung - in Deutschland (noch) kaum ein Thema, in: Bär, C., Grädler, T., Mayr, R. (Eds.), Digitalisierung Im Spannungsfeld von Politik, Wirtschaft, Wissenschaft Und Recht. Springer Gabler, Berlin.

Müller, N., 2020. Es muss nicht kompliziert sein. TeSi 10, 16–18. https://doi.org/10.37544/2191-0073-2020-03-16

Myers, M.D., 2019. Qualitative Research in Business and Management 1–364.

Nather, S., 2018. Improving Information Security Through Risk Management and Enterprise Architecture Integration, in: International Conference on Cyber Warfare and Security. Academic Conferences International Limited, p. 420.

Niemimaa, E., Niemimaa, M., 2017. Information systems security policy implementation in practice: from best practices to situated practices. Eur J Inf Syst 26, 1–20. https://doi.org/10.1057/s41303-016-0025-y

Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E., Bonacina, S., 2021. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. Sensors 21, 5119. https://doi.org/10.3390/s21155119

Nikolova, I., 2017. Best Practice for Cybersecurity Capacity Building in Bulgaria's Public Sector. ISIJ 38, 79–92. https://doi.org/10.11610/isij.3806

Norris, D.F., Mateczun, L., Joshi, A., Finin, T., 2019. Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity. Public Administration Review 79, 895–904. https://doi.org/10.1111/puar.13028

Nugraha, Y., 2020. Information System Development With Comparison of Waterfall and Prototyping Models. RISTEC 1. https://doi.org/10.31980/ristec.v1i2.1202

Nunamaker Jr., J.F., Chen, M., Purdin, T.D.M., 1990. Systems Development in Information Systems Research. Journal of Management Information Systems 7, 89–106. https://doi.org/10.1080/07421222.1990.11517898

Onibere, M., Ahmad, A., Maynard, S., 2017. The Chief Information Security Officer and the Five Dimensions of a Strategist.

Onwubiko, C., Onwubiko, A., 2019. Cyber KPI for Return on Security Investment, in: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). Presented at the 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), IEEE, Oxford, United Kingdom, pp. 1–8. https://doi.org/10.1109/CyberSA.2019.8899375

OSA Landscape [WWW Document], 2024. URL https://www.opensecurityarchitecture.org/cms/foundations/osa-landscape (accessed 5.18.24).

Österle, H., Becker, J., Frank, U., Hess, T., Karagiannis, D., Krcmar, H., Loos, P., Mertens, P., Oberweis, A., Sinz, E.J., 2010. Memorandum zur gestaltungsorientierten Wirtschaftsinformatik. Schmalenbachs Z betriebswirtsch Forsch 62, 664–672. https://doi.org/10.1007/BF03372838

Oswald, G., Krcmar, H. (Eds.), 2018. Digitale Transformation: Fallbeispiele und Branchenanalysen, Informationsmanagement und digitale Transformation. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-22624-4

OZG - Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen, n.d.

Paech, A., Vogel, D., 2022. IT-Führungsrollen des Top-Management-Teams im öffentlichen Sektor. HMD 59, 854–866. https://doi.org/10.1365/s40702-022-00873-w

Park, S.-K., Lee, S.-H., Kim, T.-Y., Jun, H.-J., Kim, T.-S., 2017. A performance evaluation of information security training in public sector. J Comput Virol Hack Tech 13, 289–296. https://doi.org/10.1007/s11416-017-0305-7

Paulsen, C., Byers, R., 2019. Glossary of key information security terms (No. NIST IR 7298r3). National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.IR.7298r3

Peffers, K., Tuunanen, T., Gengler, C.E., Rossi, M., Hui, W., 2006. THE DESIGN SCIENCE RESEARCH PROCESS: A MODEL FOR PRODUCING AND PRESENTING INFORMATION SYSTEMS RESEARCH.

Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S., 2007. A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems 24, 45–77. https://doi.org/10.2753/MIS0742-1222240302

Petrlic, R., Sorge, C., Ziebarth, W., 2022. Datenschutz: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-39097-6

Pfeiffer, S., Seiffert, M., 2019. Security-Management-as-a-Service. Datenschutz Datensich 43, 23–27. https://doi.org/10.1007/s11623-019-1055-0

Pfeiffer, U., 2022. Eine starke Unternehmenskultur minimiert Cyberrisiken. Digitale Welt 6, 24–27. https://doi.org/10.1007/s42354-022-0429-x

Phelps, M., 2021. The role of the private sector in counter-terrorism: a scoping review of the literature on emergency responses to terrorism. Secur J 34, 599–620. https://doi.org/10.1057/s41284-020-00250-6

Ploder, A., Hamann, J., 2021. Practices of Ethnographic Research: Introduction to the Special Issue. Journal of Contemporary Ethnography 50, 3–10. https://doi.org/10.1177/0891241620979100

Poehlmann, N., Caramancion, K.M., Tatar, I., Li, Y., Barati, M., Merz, T., 2021. The

Organizational Cybersecurity Success Factors: An Exhaustive Literature Review, in: Daimi, K., Arabnia, H.R., Deligiannidis, L., Hwang, M.-S., Tinetti, F.G. (Eds.), Advances in Security, Networks, and Internet of Things, Transactions on Computational Science and Computational Intelligence. Springer International Publishing, Cham, pp. 377–395. https://doi.org/10.1007/978-3-030-71017-0_27

Pohlmann, N., 2022. Cyber-Sicherheit: das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung, 2. Auflage. ed. Springer Vieweg, Wiesbaden [Heidelberg]. https://doi.org/10.1007/978-3-658-36243-0

Pohlmann, N., 2019. Cyber-Sicherheit: das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung. Springer Vieweg, Wiesbaden.

Pohlmann, N., 2018. Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung, in: Bär, C., Grädler, T., Mayr, R. (Eds.), Digitalisierung Im Spannungsfeld von Politik, Wirtschaft, Wissenschaft Und Recht. Springer Gabler, Berlin.

Potter, D.O., Hurley, J.S., 2020. The new role of the “Next generation” CFO. Presented at the Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020, pp. 398–401. https://doi.org/10.34190/ICCWS.20.096

Preis, B., Susskind, L., 2022. Municipal Cybersecurity: More Work Needs to be Done. Urban Affairs Review 58, 614–629. https://doi.org/10.1177/1078087420973760

Preußig, J., 2018. Agiles Projektmanagement: Scrum, Use Cases, Task Boards & Co. Haufe-Lexware.

Pries-Heje, J., Baskerville, R., Venable, J., 2007. Soft Design Science Research: The 2nd International Conference on Design Science Research in IT (DESRIST). Proceedings from the 2nd International Conference on Design Science Research in IT (DESRIST) 18–38.

Raising Awareness of Cybersecurity [WWW Document], 2022. . ENISA. URL https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity (accessed 12.14.22).

Rajivan, P., Cooke, N., 2017. Impact of Team Collaboration on Cybersecurity Situational Awareness, in: Liu, P., Jajodia, S., Wang, C. (Eds.), Theory and Models for Cyber Situation Awareness, Lecture Notes in Computer Science. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-61152-5

Rawindaran, N., Jayal, A., Prakash, E., Hewage, C., 2023. Perspective of small and medium enterprise (SME’s) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. International Journal of Information Management Data Insights 3, 100191. https://doi.org/10.1016/j.jjimei.2023.100191

Recker, J., 2021. Scientific research in information systems: a beginner’s guide, Second edition. ed, Progress in IS. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-030-85436-2

Rehbohm, T., Kalmbach, P., 2022. MMR-Aktuell 2021, 438461 - beck-online, Grundforderungen von Informations- und Cybersicherheit in Ländern [WWW Document]. URL https://beck-online.beck.de/?vpath=bibdata/zeits/MMRAktuell/2021/438461.htm (accessed 9.8.22).

Rehbohm, T., Kalmbach, P.L., 2023. Herausforderungen der föderalen Cybersicherheit vs. Änderung in der Bund-Länder Gewaltenteilung. Datenschutz Datensich 47, 338–342. https://doi.org/10.1007/s11623-023-1772-2

Rehbohm, T., Kemmerich, R., Cap, C.H., Sandkuhl, K., 2022a. Sicherheitsmanagement, Cybersicherheit und Daseinsvorsorge: Empirische Studie in deutschen Kommunen. Datenschutz Datensich 46, 448–454. https://doi.org/10.1007/s11623-022-1637-0

Rehbohm, T., Sandkuhl, K., Cap, C.H., Kemmerich, T., 2022b. Integrated Security Management of Public and Private Sector for Critical Infrastructures – Problem Investigation, in: Abramowicz, W., Auer, S., Stróżyna, M. (Eds.), Business Information Systems Workshops, Lecture Notes in Business Information Processing. Springer International Publishing, Cham, pp. 291–303. https://doi.org/10.1007/978-3-031-04216-4_26

Rehbohm, T., Sandkuhl, K., Kemmerich, T., 2021. On Challenges of Cyber and Information Security Management in Federal Structures - The Example of German Public Administration. p. 13.

Reinders, H., Ditton, H., 2011. Überblick über Forschungsmethoden, in: Reinders, H., Ditton, Hartumut, Gräsel, C., Gniewosz, B. (Eds.), Empirische Bildungsforschung. 2: Strukturen und Methoden. S.l.

Reiss, M., 2018. Dokumentationsmanagement – Basis für IT-Governance: 11 Schritte zur IT-Dokumentation. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-19847-3

Reiss, M., Reiss, G., 2018. Praxisbuch IT-Dokumentation: Vom Betriebshandbuch bis zum Dokumentationsmanagement – die Dokumentation im Griff. Carl Hanser Verlag GmbH Co KG.

Remy, J., Stettner, R., 2021. Cybersicherheit als Aufgabe der Länder. Datenschutz Datensich 45, 254–258. https://doi.org/10.1007/s11623-021-1429-y

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), 2022. , OJ L.

Riege, C., Saat, J., Bucher, T., 2009. Systematisierung von Evaluationsmethoden in der gestaltungsorientierten Wirtschaftsinformatik, in: Becker, J., Krcmar, H., Niehaves, B. (Eds.), Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik. Physica-Verlag HD, Heidelberg, pp. 69–86. https://doi.org/10.1007/978-3-7908-2336-3_4

Riek, M., Bohme, R., Moore, T., 2016. Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. IEEE Transactions on Dependable and Secure Computing 13, 261–273. https://doi.org/10.1109/TDSC.2015.2410795

Robra-Bissantz, S., Strahringer, S., 2020. Wirtschaftsinformatik-Forschung für die Praxis. HMD 57, 162–188. https://doi.org/10.1365/s40702-020-00603-0

Roggenbach, M., Cerone, A., Schlingloff, B.-H., Schneider, G., Shaikh, S.A., 2022. Formal Methods for Software Engineering: Languages, Methods, Application Domains, Texts in Theoretical Computer Science. An EATCS Series. Springer International Publishing, Cham. https://doi.org/10.1007/978-3-030-38800-3

Rohr, M., 2015. Sicherheit von Webanwendungen in der Praxis: Wie sich Unternehmen schützen können – Hintergründe, Maßnahmen, Prüfverfahren und Prozesse. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-03851-9

Rohrer, A., Söllner, D., 2017. IT-Service-Management mit FitSM: ein praxisorientiertes und leichtgewichtiges Framework für die IT, 1. Auflage. ed. dpunkt.verlag, Heidelberg.

Romanovská, F., Piter, T., 2022. Multi-level cybersecurity gevernance frameworks for

public administration. IDIMT-2022 Digitalization of society business and management in a pandemic; 30th Interdisciplinary Information Management Talk / Chroust. https://doi.org/10.35011/IDIMT-2022-277

Rosemann, M., Vessey, I., 2008. Toward Improving the Relevance of Information Systems Research to Practice: The Role of Applicability Checks. MIS Quarterly 32, 1–22.

Rosner, S., Gombos, G., 2007. Systemaufstellung als Aktionsforschung: Grundlagen, Anwendungsfelder, Perspektiven, 1. Aufl. ed, Systemische Organisationsberatung und Aktionsforschung. Hampp, München Mering.

Rossi, M., Stein, M., 2003. Design Research Workshop: A Proactive Approach, in: 26th Information System Research Seminar in Scandinavia. The IRIS Association.

Rost, M., Pfitzmann, A., 2009. Datenschutz-Schutzziele — revisited. DuD 33, 353–358. https://doi.org/10.1007/s11623-009-0072-9

Sabtu, S.B.M., Mohamad, K.M., 2021. Critical Information Infrastructure Protection Requirement for the Malaysian Public Sector, in: Saeed, F., Al-Hadhrami, T., Mohammed, F., Mohammed, E. (Eds.), Advances on Smart and Soft Computing, Advances in Intelligent Systems and Computing. Springer, Singapore, pp. 371–381. https://doi.org/10.1007/978-981-15-6048-4_32

Salas, E., DiazGranados, D., Klein, C., Burke, C.S., Stagl, K.C., Goodwin, G.F., Halpin, S.M., 2008. Does Team Training Improve Team Performance? A Meta-Analysis. Hum Factors 50, 903–933. https://doi.org/10.1518/001872008X375009

Sallos, M.P., Garcia-Perez, A., Bedford, D., Orlando, B., 2019. Strategy and organisational cybersecurity: a knowledge-problem perspective. Journal of Intellectual Capital 20, 581–597. https://doi.org/10.1108/JIC-03-2019-0041

Savold, R., Dagher, N., Frazier, P., McCallam, D., 2017. Architecting Cyber Defense: A Survey of the Leading Cyber Reference Architectures and Frameworks, in: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud). Presented at the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE, New York, NY, USA, pp. 127–138. https://doi.org/10.1109/CSCloud.2017.37

Schaberreiter, T., 2022. A Case for Cybersecurity Awareness Systems, in: Andriessen, J., Schaberreiter, T., Papanikolaou, A., Röning, J. (Eds.), Cybersecurity Awareness, Advances in Information Security. Springer International Publishing, Cham, pp. 161–181. https://doi.org/10.1007/978-3-031-04227-0_7

Schallbruch, M., 2018. Schwacher Staat im Netz: wie die Digitalisierung den Staat in Frage stellt. Springer, Wiesbaden.

Schallbruch, M., 2017. IT-Sicherheitsrecht – Schutz kritischer Infrastrukturen und staatlicher IT-Systeme. Computer und Recht 33. https://doi.org/10.9785/cr-2017-1007

Schardt, M., 2017. Der IT-Planungsrat – Zentrum der Digitalisierung der öffentlichen Verwaltung?! VM 23, 227–235. https://doi.org/10.5771/0947-9856-2017-5-227

Schefferlie, J., 2020. THE IMPACT OF PROJECTS AND PROJECT MANAGEMENT WILL INCREASE. European Project Management Journal 10, 72–75.

Schenk, B., Dietrich, A., 2018. Die Digitale Transformation als Disruption der öffentlichen Verwaltung, in: Arnold, C., Knödler, H. (Eds.), Die informatisierte Service-Ökonomie. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-21528-6

Schläger, U., Thode, J.-C., 2022. Handbuch Datenschutz und IT-Sicherheit. Erich Schmidt

Verlag GmbH & Co. KG, Berlin. https://doi.org/10.37307/b.978-3-503-20534-9

Schmid, A. (Ed.), 2019. Verwaltung, eGovernment und Digitalisierung: Grundlagen, Konzepte und Anwendungsfälle. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-27029-2

Schmitz-Berndt, S., Chiara, P.G., 2022. One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. Int. Cybersecur. Law Rev. 3, 289–311. https://doi.org/10.1365/s43439-022-00058-7

Scholl, M., 2018. Was haben Informationssicherheit, Bewusstsein, öffentliche Verwaltung und Frauen miteinander zu tun?, in: Beck, J., Stember, J. (Eds.), Perspektiven der angewandten Verwaltungsforschung in Deutschland. Nomos Verlagsgesellschaft mbH & Co. KG, pp. 159–180. https://doi.org/10.5771/9783845296869-159

Schönbohm, A., 2018. Flexibilität und Unabhängigkeit - Rahmenbedingungen für eine gesellschaftliche Cyber-Sicherheit, in: Bär, C., Grädler, T., Mayr, R. (Eds.), Digitalisierung Im Spannungsfeld von Politik, Wirtschaft, Wissenschaft Und Recht. Springer Gabler, Berlin.

Schreiber, L., 2022. Rechtliche Implikationen von Cybersicherheitsvorfällen in der kommunalen Verwaltung. Gesellschaft für Informatik, Bonn. https://doi.org/10.18420/inf2022_22

Schreyögg, G., Geiger, D., 2016. Organisation: Grundlagen moderner Organisationsgestaltung. Mit Fallstudien. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-8349-4485-6

Schubert, P., Bhaskaran, K., 2007. The eXperience Methodology for Writing IS Case Studies. AMCIS 2007 Proceedings 16.

Schulte, M., Schröder, R. (Eds.), 2011. Handbuch des Technikrechts. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-11884-5

Schulz, G., 2015. Informationssicherheit in Kommunen: Voraussetzung für den Datenschutz der Bürgerinnen und Bürger. Datenschutz Datensich 39, 466–471. https://doi.org/10.1007/s11623-015-0451-3

Schumpeter, J., Becker, M.C., Knudsen, T., 2002. New Translations: Theorie der wirtschaftlichen Entwicklung. The American Journal of Economics and Sociology 61, 405–437.

Schünemann, W., J., 2020. Cybersicherheit, in: Klenk, T., Nullmeier, F., Wewer, G. (Eds.), Handbuch Digitalisierung in Staat und Verwaltung. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-23668-7

Schwab, C., Bogumil, J., Kuhlmann, S., Gerber, S., 2020. Digitalisierung von Verwaltungsleistungen in Bürgerämtern, in: Klenk, T., Nullmeier, F., Wewer, G. (Eds.), Handbuch Digitalisierung in Staat und Verwaltung. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-23668-7

Schwarzer, E., 2018. Das Dilemma der Politik in der digitalen Welt, in: Bär, C., Grädler, T., Mayr, R. (Eds.), Digitalisierung Im Spannungsfeld von Politik, Wirtschaft, Wissenschaft Und Recht. Springer Gabler, Berlin.

Seckelmann, M., Brunzel, M., 2021a. Das Onlinezugangsgesetz im Kontext einer digital vernetzten Gesellschaft und datengetriebenen Wirtschaft: Zur Einleitung, in: Seckelmann, M., Brunzel, M. (Eds.), Handbuch Onlinezugangsgesetz: Potenziale - Synergien - Herausforderungen. Springer, Berlin.

Seckelmann, M., Brunzel, M. (Eds.), 2021b. Handbuch Onlinezugangsgesetz: Potenziale - Synergien - Herausforderungen. Springer, Berlin.

Seibel, W., 2018. Verwaltung, in: Voigt, R. (Ed.), Handbuch Staat. Springer Fachmedien Wiesbaden, Wiesbaden, pp. 1279–1288. https://doi.org/10.1007/978-3-658-20744-1_115

Sengupta, A., 2022. A Stakeholder-Centric Approach for Defining Metrics for Information Security Management Systems, in: Luo, B., Mosbah, M., Cuppens, F., Ben Othmane, L., Cuppens, N., Kallel, S. (Eds.), Risks and Security of Internet and Systems, Lecture Notes in Computer Science. Springer International Publishing, Cham, pp. 57–73. https://doi.org/10.1007/978-3-031-02067-4_4

Shayo, C., Lin, F., 2019. An Exploration of the Evolving Reporting Organizational Structure for the Chief Information Security Officer (CISO) Function. JCSIT 7. https://doi.org/10.15640/jcsit.v6n2a1

Siau, K., Rossi, M., 1998. Evaluation of information modeling methods-a review, in: Proceedings of the Thirty-First Hawaii International Conference on System Sciences. Presented at the Proceedings of the Thirty-First Hawaii International Conference on System Sciences, pp. 314–322 vol.5. https://doi.org/10.1109/HICSS.1998.648327

Sidorova, A., Evangelopoulos, N., Valacich, J.S., Ramakrishnan, T., 2008. Uncovering the Intellectual Core of the Information Systems Discipline. MIS Quarterly 32, 467–482. https://doi.org/10.2307/25148852

Silva, L., Hsu, C., Backhouse, J., McDonnell, A., 2016. Resistance and power in a security certification scheme: The case of *c:cure*. Decision Support Systems, A Comprehensive Perspective on Information Systems Security - Technical Advances and Behavioral Issues 92, 68–78. https://doi.org/10.1016/j.dss.2016.09.014

Simon, D., Fischbach, K., Schoder, D., 2014. Enterprise architecture management and its role in corporate strategic management. Inf Syst E-Bus Manage 12, 5–42. https://doi.org/10.1007/s10257-013-0213-4

Simonson, R.J., Keebler, J.R., Lessmiller, M., Richards, T., Lee, J.C., 2020. Cybersecurity Teamwork: A Review of Current Practices and Suggested Improvements. Proceedings of the Human Factors and Ergonomics Society Annual Meeting 64, 451–455. https://doi.org/10.1177/1071181320641101

Siponen, M., Willison, R., 2009. Information security management standards: Problems and solutions. Information & Management 46, 267–270. https://doi.org/10.1016/j.im.2008.12.007

Solms, R. von, Niekerk, J. van, 2013. Form information security to cyber security 97–102.

Sonnenberg, C., vom Brocke, J., 2012. Evaluations in the Science of the Artificial – Reconsidering the Build-Evaluate Pattern in Design Science Research, in: Peffers, K., Rothenberger, M., Kuechler, B. (Eds.), Design Science Research in Information Systems. Advances in Theory and Practice, Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, pp. 381–397.

Sowa, A., 2017. Management der Informationssicherheit: Kontrolle und Optimierung, Studienbücher Informatik. Springer Vieweg, Wiesbaden; [Heidelberg]. https://doi.org/10.1007/978-3-658-15627-5

Sowa, A., Rost, M., 2020. Die ISO 27701 und das SDM-V2 im Lichte der Umsetzung der DSGVO. Datenschutz Datensich 44, 659–662. https://doi.org/10.1007/s11623-020-1344-7

Spindler, G., 2021. Cybersecurity und Unternehmensleitung, in: Bittner, M.-P., Guntermann, A., Müller, C.B., Rostam, D. (Eds.), Cybersecurity als Unternehmensleitungsaufgabe. Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783748927679

Stasser, G., Titus, W., 1987. Effects of information load and percentage of shared information on the dissemination of unshared information during group discussion. Journal of Personality and Social Psychology 53, 81–93. https://doi.org/10.1037/0022-3514.53.1.81

Steinmann, H., Schreyögg, G., 2000. Management: Grundlagen der Unternehmensführung, 5. überarbeitete Auflage. ed. Wiesbaden.

Stoner, J.A.F., 1961. A comparison of individual and group decisions involving risk (PhD Thesis). Massachusetts Institute of Technology.

Strübing, J., 2021. Grounded Theory: Zur sozialtheoretischen und epistemologischen Fundierung eines pragmatistischen Forschungsstils. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-24425-5

Studier, R., epubli GmbH, 2021. Sozialgesetzbuch Fünftes Buch (SGB V) Gesetzliche Krankenversicherung.

Susukailo, V., Opirsky, I., Yaremko, O., 2022. Methodology of ISMS Establishment Against Modern Cybersecurity Threats, in: Klymash, M., Beshley, M., Luntovskyy, A. (Eds.), Future Intent-Based Networking, Lecture Notes in Electrical Engineering. Springer International Publishing, Cham, pp. 257–271. https://doi.org/10.1007/978-3-030-92435-5_15

Symmank, C., Hoffmann, S., 2017. Leugnung und Ablehnung von Verantwortung, in: Heidbrink, L., Langbehn, C., Loh, J. (Eds.), Handbuch Verantwortung. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-06110-4

Taddeo, M., 2019. Is Cybersecurity a Public Good? Minds & Machines 29, 349–354. https://doi.org/10.1007/s11023-019-09507-5

Takeda, H., Veerkamp, P., Yoshikawa, H., 1990. Modeling Design Process. AI Magazine 11, 37–37. https://doi.org/10.1609/aimag.v11i4.855

Tatiara, R., Fajar, A.N., Siregar, B., Gunawan, W., 2018. Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001. J. Phys.: Conf. Ser. 978, 012039. https://doi.org/10.1088/1742-6596/978/1/012039

Tornatzky, L.G., Fleischer, M., Chakrabarti, A.K., 1990. processes of technological innovation. Lexington Books.

Totok, A., 2016. Von der Business-Intelligence-Strategie zum Business Intelligence Competency Center, in: Gluchowski, P., Chamoni, P. (Eds.), Analytische Informationssysteme: Business Intelligence-Technologien und -Anwendungen. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-47763-2

Vahs, D., 2015. Organisation: ein Lehr- und Managementbuch, 9., überarbeitete und erweiterte Auflage. ed. Schäffer-Poeschel Verlag, Stuttgart.

van Steen, T., Deeleman, J.R.A., 2021. Successful Gamification of Cybersecurity Training. Cyberpsychology, Behavior, and Social Networking 24, 593–598. https://doi.org/10.1089/cyber.2020.0526

Venable, J., Pries-Heje, J., Baskerville, R., 2016. FEDS: a Framework for Evaluation in Design Science Research. Eur J Inf Syst 25, 77–89. https://doi.org/10.1057/ejis.2014.36

Venable, J., Pries-Heje, J., Baskerville, R., 2012. A Comprehensive Framework for Evaluation in Design Science Research, in: Peffers, K., Rothenberger, M., Kuechler, B. (Eds.), Design Science Research in Information Systems. Advances in Theory and Practice, Lecture Notes in Computer Science. Springer, Berlin, Heidelberg, pp. 423–438. https://doi.org/10.1007/978-3-642-29863-9_31

Venkatesh, V., Brown, S.A., Bala, H., 2013. Bridging the Qualitative-Quantitative Divide:

Guidelines for Conducting Mixed Methods Research in Information Systems. MIS Quarterly 37, 21–54.

Vitak, J., Crouse, J., LaRose, R., 2011. Personal Internet use at work: Understanding cyberslacking. Computers in Human Behavior, 2009 Fifth International Conference on Intelligent Computing 27, 1751–1759. https://doi.org/10.1016/j.chb.2011.03.002

Völker, J.C., 2012. IT-Infrastructure Library (ITIL) Für Die Kommunalverwaltung Unter Besonderer Berücksichtigung der Kleinen und Mittleren Gemeinden in Baden-Württemberg. Logos Verlag Berlin GmbH.

vom Brocke, J., Hevner, A., Maedche, A., 2020. Introduction to Design Science Research, in: vom Brocke, J., Hevner, A., Maedche, A. (Eds.), Design Science Research. Cases, Progress in IS. Springer International Publishing, Cham, pp. 1–13. https://doi.org/10.1007/978-3-030-46781-4_1

vom Brocke, J., Simons, A., Niehaves, B., Reimer, K., 2009. RECONSTRUCTING THE GIANT: ON THE IMPORTANCE OF RIGOUR IN DOCUMENTING THE LITERATURE SEARCH PROCESS.

Von Faber, E., Behnsen, W., 2018. Joint Security Management: organisationsübergreifend handeln, Edition <kes>. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-20834-9

von Lucke, J., 2021. Die Wissenschaft Verwaltungsinformatik und das Onlinezugangsgesetz, in: Seckelmann, M., Brunzel, M. (Eds.), Handbuch Onlinezugangsgesetz: Potenziale - Synergien - Herausforderungen. Springer, Berlin.

von Salden, P., Schäfer, L.W., 2018. Von Asymmetrien und Unsicherheiten im Cyber-Raum - Cyber-Sicherheit als gesamtstaatliche Aufgabe, in: Bär, C., Grädler, T., Mayr, R. (Eds.), Digitalisierung Im Spannungsfeld von Politik, Wirtschaft, Wissenschaft Und Recht. Springer Gabler, Berlin.

von Solms, B., 2000. Information Security — The Third Wave? Computers & Security 19, 615–620. https://doi.org/10.1016/S0167-4048(00)07021-8

Von Solms, B., Von Solms, R., 2004. The 10 deadly sins of information security management. Computers & Security 23, 371–376. https://doi.org/10.1016/j.cose.2004.05.002

von Solms, R., 1999. Information security management: why standards are important. Information Management & Computer Security 7, 50–58. https://doi.org/10.1108/09685229910255223

von Solms, R., 1996. Information security management: The second generation. Computers & Security 15, 257–265. https://doi.org/10.1016/0167-4048(96)88939-5

Wächter, L., 2017. Ökonomen auf einen Blick. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-14307-7

Wahl, D., 2013. Lernumgebungen erfolgreich gestalten: vom trägen Wissen zum kompetenten Handeln ; mit Methodensammlung. Julius Klinkhardt.

Walls, J.G., Widmeyer, G.R., El Sawy, O.A., 1992. Building an Information System Design Theory for Vigilant EIS. Information Systems Research 3, 36–59. https://doi.org/10.1287/isre.3.1.36

Walsham, G., 2006. Doing interpretive research. European Journal of Information Systems 15, 320–330. https://doi.org/10.1057/palgrave.ejis.3000589

Watson, R.T., Webster, J., 2020. Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0. Journal of Decision Systems 29, 129–147.

https://doi.org/10.1080/12460125.2020.1798591

Weber, A., Heiser, G., Kuhlmann, D., Schallbruch, M., Chattopadhyay, A., Guilley, S., Kasper, M., Krauß, C., Krüger, P.S., Reith, S., Seifert, J.-P., 2020. Sichere IT ohne Schwachstellen und Hintertüren. TATuP 29, 30–36. https://doi.org/10.14512/tatup.29.1.30

Weber, Karsten, Christen, M., Herrmann, D., 2020. Bedrohung, Verwundbarkeit, Werte und Schaden: Cyberattacken und Cybersicherheit als Thema der Technikfolgenabschätzung. TATuP 29, 11–15. https://doi.org/10.14512/tatup.29.1.11

Weber, K., Schütz, A.E., Fertig, T., 2019. Grundlagen und Anwendung von Information Security Awareness: Mitarbeiter zielgerichtet für Informationssicherheit sensibilisieren, essentials. Springer Fachmedien Wiesbaden, Wiesbaden. https://doi.org/10.1007/978-3-658-26258-7

Weber, Kristin, Veit, D., Johannsen, A., 2020. Anforderungen an die IT-Dokumentation aus Sicht von Informationssi- cherheit und Datenschutz. 33. AKWI Jahrestagung.

Weber, W.W., 2004. Innovation durch Injunktion - Warum man Innovationen nicht planen (lassen) kann. Sordon, Göttingen.

Webster, J., Watson, R.T., 2002. Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly 26, xiii–xxiii.

Weissmann, P., 2023. Die neue EU NIS 2 Direktive für Cyber Security in KRITIS [WWW Document]. URL https://www.openkritis.de/it-sicherheitsgesetz/eu-nis-2-direktive-kritis.html (accessed 5.9.23).

Werner, C., Brinker, N., Raabe, O., 2022. Grundlagen für ein gesetzliches IT-Sicherheitsrisikomanagement — Ansätze zur Vereinheitlichung von Rollenmodell, Risikomanagement und Definitionen für das IT-Sicherheitsrecht. Computer und Recht 38, 817–824. https://doi.org/10.9785/cr-2022-381219

Whitten, D., 2008. The Chief Information Security Officer: An Analysis of the Skills Required for Success. Journal of Computer Information Systems.

Wilde, T., Hess, T., 2006. Methodenspektrum der Wirtschaftsinformatik: Überblick und Portfoliobildung.

Wimmer, M.A., 2021. Once-Only und Digital First als Gestaltungsprinzipien der vernetzten Verwaltung von morgen, in: Seckelmann, M., Brunzel, M. (Eds.), Handbuch Onlinezugangsgesetz: Potenziale - Synergien - Herausforderungen. Springer, Berlin.

Wind, M., 2006. IT in der Verwaltung – lange Historie, neue Perspektiven, in: Wind, M., Kröger, D. (Eds.), Handbuch IT in der Verwaltung: mit 16 Tab. Springer, Berlin Heidelberg.

Windoffer, A., 2018. Herausforderungen der Digitalisierung aus der Perspektive der öffentlichen Verwaltung, in: Bär, C., Grädler, T., Mayr, R. (Eds.), Digitalisierung Im Spannungsfeld von Politik, Wirtschaft, Wissenschaft Und Recht. Springer Gabler, Berlin.

Wirtz, B.W., Weyerer, J.C., 2017. Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats. International Journal of Public Administration 40, 1085–1100. https://doi.org/10.1080/01900692.2016.1242614

Wollinger, G.R., Schulze, A., 2020. Handbuch Cybersecurity für die öffentliche Verwaltung. Kommunal- und Schul-Verlag.

Wong, C.K., Maynard, S.B., Ahmad, A., Naseer, H., 2020. Information Security Governance: A Process Model and Pilot Case Study. Information Security Governance.

Yin, R.K., 1981. The Case Study Crisis: Some Answers. Administrative Science Quarterly 26, 58. https://doi.org/10.2307/2392599

Yoo, C.W., Goo, J., Rao, H.R., 2020. Is Cybersecurity a Team Sport? A Multilevel Examination of Workgroup Information Security Effectiveness. MISQ 44, 907–931. https://doi.org/10.25300/MISQ/2020/15477

Zakaria, K.N., Zainal, A., Othman, S.H., Kassim, M.N., 2019. Feature Extraction and Selection Method of Cyber-Attack and Threat Profiling in Cybersecurity Audit, in: 2019 International Conference on Cybersecurity (ICoCSec). Presented at the 2019 International Conference on Cybersecurity (ICoCSec), IEEE, Negeri Sembilan, Malaysia, pp. 1–6. https://doi.org/10.1109/ICoCSec47621.2019.8970786

Zerres, C. (Ed.), 2021. Handbuch Marketing-Controlling: Grundlagen – Methoden – Umsetzung. Springer Berlin Heidelberg, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-62837-9

Zheng, K., Albert, L.A., Luedtke, J.R., Towle, E., 2019. A budgeted maximum multiple coverage model for cybersecurity planning and management. IISE Transactions 51, 1303–1317. https://doi.org/10.1080/24725854.2019.1584832

Zwilling, M., 2022. Trends and Challenges Regarding Cyber Risk Mitigation by CISOs—A Systematic Literature and Experts' Opinion Review Based on Text Analytics. Sustainability 14, 1311. https://doi.org/10.3390/su14031311

15 Eidesstattliche Erklärung / Statutory Declaration

15.1 Eidesstattliche Erklärung

Hiermit erkläre ich, dass ich die vorliegende Dissertation mit dem Titel

Prozedurales Vorgehensmodell zum Aufbau eines ISMS
in kleinen Kommunalverwaltungen

selbständig und ohne fremde Hilfe verfasst und angefertigt habe. Es wurden nur die in der Arbeit ausdrücklich benannten Quellen und Hilfsmittel benutzt. Wörtlich oder sinngemäß übernommenes Gedankengut habe ich als solches kenntlich gemacht. Diese Dissertation wurde bisher weder im Ausland noch im Inland in gleicher oder ähnlicher Form einer anderen Prüfungsbehörde vorgelegt.

Mir ist bewusst, dass bei Abgabe einer falschen Erklärung die Prüfung als nicht bestanden zu gelten hat.

15.2 Statutory Declaration

I hereby declare that I have written the present dissertation thesis with the title

Procedural Model for the Adoption of an ISMS
in Small Public Sector Organisations

independently and without outside help. Only the sources and aids explicitly mentioned in the thesis were used. I have marked ideas taken literally or by analogy as such. So far, this dissertation has not been submitted in the same or similar form to another examination authority either abroad or in Germany.

I am aware that if a false declaration is made, the exam will be deemed failed.

Rostock, den 29.07.2024

Frank Moses

Closing words...

It always seems impossible until it’s done.

Nelson Mandela

Lebenslauf

Personalien

Name	Frank Moses
Adresse und Kontaktdaten	Otto-Hahn-Str. 9 66132 Saarbrücken eMail: frank.moses@uni-rostock.de
Geburtstag	15.06.1968
Nationalität	Deutsch
Beruf Aktuelle Dienststelle	Beamter (Ministerialrat) Unabhängiges Datenschutzzentrum des Saarlandes

Ausbildung / Wehrdienst / Studium

	Abschluss
Studium	M.Sc. (Wirtschaftswissenschaften) (2007)
Studium	Dipl.-Informatiker (1994)
Wehrdienst	Aufklärungsbatallion 8, Freyung (Bayern) 1989-1990
Berufsausbildung	Datenverarbeitungskaufmann 1987-1989
Hochschulreife	1987

Berufserfahrung

Zusammenfassung

2019 bis 2025:

Promotionsstudium an der Universität Rostock, Lehrstuhl Prof. Dr. Kurt Sandkuhl

2018 bis heute:

Unabhängiges Datenschutzzentrum des Saarlandes

Leiter Referat 4 – Technischer Datenschutz

2013-2018:

Ministerium für Finanzen

Stabsstelle für Informationssicherheit

Landesbeauftragter für Informationssicherheit (Landes-CISO)

Leitung zweier Arbeitsgruppen des IT-Planungsrats der Bundesrepublik (AG-ISMS und AG-Maturity)

1999 bis 2013:

Ministerium für Finanzen

Referent mit verschiedenen Aufgaben

1995 bis 1999:

Ministerium für Wirtschaft

Mitarbeiter im IT-Referat

Saarbrücken, den 29.07.2024