Complex Systems Informatics and Modeling Quarterly (CSIMQ)
eISSN: 2255-9922
Published online by RTU Press, https://csimq-journals.rtu.lv
Article 204, Issue 37, December 2023/January 2024, Pages 54–68
https://doi.org/10.7250/csimq.2023-37.03

Information Security Management in Small Public Sector Organizations: Requirements and Design of a Procedural Approach

Frank Moses[1 *] and Kurt Sandkuhl[1, 2]

[1] University of Rostock, Albert-Einstein-Str. 22, 18059 Rostock, Germany
[2] Jönköping University, Box 1026, 55111 Jönköping, Sweden

frank.moses@uni-rostock.de, kurt.sandkuhl@uni-rostock.de

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 an essential aspect 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 the development of 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 and complements them with the obstacles and reasons for success in the introduction of 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.
Keywords: Hindering Factors, Requirements, Information Security, ISMS.

1 Introduction

The dependency on technology for almost every single process in an organization has put information security management systems (ISMSs) 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.

* Corresponding author

Reference: F. Moses and K. Sandkuhl, "Information Security Management in Small Public Sector Organizations: Requirements and Design of a Procedural Approach," Complex Systems Informatics and Modeling Quarterly, CSIMQ, no. 37, pp. 54–68, 2023. Available: https://doi.org/10.7250/csimq.2023-37.03

Additional information. Author ORCID iD: F. Moses – https://orcid.org/0009-0008-8117-7233, K. Sandkuhl – https://orcid.org/0000-0002-7431-8412. PII S225599222300204X. Received: 11 February 2023. Accepted: 18 December 2023. Available online: 30 December 2023.

The information belonging to sensitive and critical organizations must be secured. Malicious cyber activities mainly take the form of business disruption, data and property destruction, and theft of financial or sensitive data [1, 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 in the public sector [2, p. 710], [3, p. 148].

The focus of this article[†] 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 organizational units of the public sector (SPSO). Against this background, the main obstacles to the implementation of an ISMS in SPSOs are gathered from the literature and a foundation for the creation of a first approach of a procedural model is derived from this.

In many centralized governmental structures, there are guidelines, recommendations, or even mandatory standards for setting up and operating an ISMS. However, in small federal governmental structures, this is often not the case [4] which establishes the responsibility for ISMS on the individual organisational unit. Furthermore, these organizations are heterogeneous in size, structure, administrative tasks, responsibilities, and resource availability. Due to this diversity, many general approaches for ISMS are not applicable. This also coincides with the author's experiences of more than 25 years in a leading position in ministerial administration.

The goal of our research is 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 [5] should be considered. The article is structured as follows:

Section 2 "Methodology" describes the phases of the research paradigm used in this work, the Design Science approach, and summarizes the results so far. Section 3 summarizes the investigation into problem relevance that was conducted in a previous work.

Section 4 "Identifying the requirements for the adoption and diffusion of an ISMS" is divided into 3 subsections. The first subsection presents the identification of the requirements that can be derived for the SPSO from the NIS-2 guideline. The second subsection contributes 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, the NIS-2 requirements and the requirements from the literature are compared and integrated. These results are structured in a further step to develop a rough process model, which is derived from the requirements and described in Section 5. This process model has already been successfully tested in an artificial environment. Currently, the procedure model is being tested in a real environment with different test subjects. Section 6 summarizes the work and discusses limitations and future work.

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) [6]. DSR is a research paradigm aiming at problem-solving in organizational settings with a focus on developing valid and reliable knowledge for designing the required solutions. DSR research projects typically consist of several phases and require the use of different research methods depending on the DSR phase and intended design solution.

This article concerns the phase requirements definition, design, and development of the design solution, i.e., the core artefact. Table 1 provides an overview of the research activities performed in the different phases of the DSR process, the research methods used for these activities, the results achieved, and the sections of this article providing information about the results.

[†] This article is an extended version of work presented at the 13th Workshop on Business and IT Alignment (BITA): Frank Moses and Kurt Sandkuhl (2023), "ISMS in Small Public Sector Organisations: Requirements and Design of a Procedural Approach." Proceeding BIR 2023 Workshops and Doctoral Consortium, CEUR online workshop proceedings, vol. 3514. Available: https://ceur-ws.org/Vol-3514/short60.pdf

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

DSR Phase	Research activity	Result / Artefact
Problem Investigation	A survey among small-scale organizations to confirm relevance	Problem relevance confirmed (Section 3)
	Literature analysis to determine the state of research	Inhibiting factors and critical success factors visible in literature and NIS2-Directive (Section 4.1)
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 (Section 4.2)
Design and develop Artifact	Conceptual-deductive work to design a Foundation of a procedural model based on requirements	Rough procedural model (Section 5)
Demonstrate	Not covered in this work	
Evaluate Artifact	Not covered in this work	

The contributions of this article are presented in Sections 4 and 5. In Section 4, we started by focusing on the requirements of the NIS-2 Directive. Furthermore, we have identified further important requirements through a literature review. We merged both lists of requirements to create an overarching list of requirements as a foundation for the development of a rough procedural model.

3 Problem Investigation and Relevance

Small and medium-sized local government organizations are increasingly the target of attacks from cyberspace [7, p. 68]. An analysis of typical problems in local governments' ISMSs confirmed this statement and also proved the relevance of our investigation into ISMSs for such organizations. More concretely, we conducted a survey among SPSOs and analyzed audit reports of their activities in information security management. The detailed results of these steps are available in [8] and can be summarized as follows:

The target group studied is facing more and more challenges, but most of them do not have defined ISMS in place; they implement basic IT security protection measures without overarching management and systematic improvement. 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 digitalization in local governments.

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 [9, pp. 86, 107] [10, p. 196].

Poor information security can lead to disruptions in the performance of tasks, reduce the performance of public authorities and, in extreme cases, bring their business processes to a standstill [11, p. 688].

In a second study, we investigated the effects of implementing an ISMS on information security in some of the SPSOs participating in the above survey. For this purpose, an initial prototype of the procedural model was applied in a field test. 24 local governments took part in the test. As a

result, it was found that a significant improvement was achieved for all of them. The detailed results are published in [4] [12, p. 656].

The above findings, as well as the studies carried out and the results associated with them, illustrate the relevance of research in the domain of small public sector organizations.

4 Identification of Requirements for the Adoption and Diffusion of ISMS

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:[13]

- **Mandatory security requirements**: Operators of critical infrastructure and digital services must implement appropriate safeguards to identify and prevent threats.
- **Security incident reporting**: Operators must report security incidents to national authorities and share information about these incidents to improve response capability.
- **Establishment of CSIRTs**: National authorities must establish Computer Security Incident Response Teams (CSIRTs) to respond to security incidents.
- **Regular security audits**: Operators must conduct regular security audits and review their security measures to ensure they are adequate and in line with current threats.
- **Cooperation between Member States**: Member States need to work together and share information to jointly 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 [14]. In Art. 21 of the NIS-2 Directive, **14 requirements** are formulated that must be met by an ISMS [13]. 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, a **strategy** must be formulated by the organisation. This is followed by the definition of **requirements** of the context. The organisational and **technical implementation** of the requirements must be coordinated by an appropriate **organizational structure** and flanked by appropriate **guidelines**. However, descriptions of the concrete implementation of an ISMS remain open [15, p. 824].

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 [3] 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 carried out 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 search terms and then with 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 of these, which were included in further analysis. The results of the search queries can be summarized as follows (Table 2):

Table 2. 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 3 presents the results of a literature review. The publications identified with this analysis were examined for factors inhibiting or supporting ISMS implementation. 60 inhibiting factors or critical success factors were identified from the literature review.

In Table 3, all 60 hindering or critical success factors are compiled. Each of them can be considered as a source of an ISMS's requirement. Behind each hindering or critical success factor, the reference is listed in brackets [*citation*] (Table 3).

On the one hand, this summary serves as the basis of this article in the sense of DSR by providing an overview of the disruptive factors of an ISMS. But also, on the other hand, it forms a foundation for further research work briefly discussed in Section 6 as not all factors are yet addressed in our research. The determined requirements that are important for this article are marked in **bold** in Table 3.

Table 3. Identified Hindering Factors resp. Critical Success Factors

Factor / Requirement	Factor / Requirement
1. **Change Management** [16]	2. Incentives (Tariff Structure) [17]
3. Application Security [18]	4. Cybersecurity Architecture [19], [20], [21]
5. Audits [16], [17], [22], [23]	6. ISMS-Organization [16], [24]
7. **Risk Management** [25], [8], [23], [26], [27], [24], [21]	8. **Education Level of Employees** [17], [28], [29], [26], [30]
9. **Awareness of Employees** [16], [17], [31], [32], [33]	10. Size of the Agency[34]
11. Disaster Recovery Planning [18]	12. Document Revision [23]
13. Self-Interest [8]	14. Achieved Level of Protection [35]
15. Control Centre (SPoC) [19], [36]	16. Misjudgement of the Management Level [25]
17. Lack of Qualified Employees [25], [31]	18. **Definition of Roles / Responsibilities and Communication** [37], [16], [26]
19. **Definition of Measures and their Implementation** [37]	20. Sanctions [17], [22] [31]
21. **Financial Resources** [16], [38], [25], [31], [34], [39]	22. **Funding** (Government) [40], [30]
23. Room for Manoeuvre [22]	24. **Business Continuity** [41]
25. Outsourcing Quota [42]	26. **Improvement process** [8]
27. Individual Attitude (Culture) [22], [32], [36]	28. Information Exchange regarding Security Vulnerabilities [37], [19], [35], [43] and Networking [19], [36]
29. Obtaining Information on Cyber Topics (OSINT) [44], [45], [26]	30. Government Interest [4]
31. **Communication** [16]	32. Concrete Measures of Security Strategies [35]
33. Continuous Improvement [37], [8]	34. Loss of Control [42], [30]
35. Cultural Context [32], [36]	36. **Leadership** [8]
37. **Policies** [16], [17], [31], [33], [37], [38], [46]–[48]	38. **Management attention** [8], [33]
39. **Integration of the Management into the Security Process** [37], [36]	40. Measurements [8]
41. **Human Factors** [17], [24], [32], [8], [49]	42. Level of the Critical Infrastructures [35]
43. **Emergency Planning** [41]	44. Organizational Perspective [41]
45. Process Management [8]	46. Productivity Loss due to Cyberloafing [22]
47. Project Management [46]	48. **Qualified Employees** [24], [25], [31], [34], [38]
49. **Legal Requirements** [4], [19]	50. Review of the Implementation of Measures [37]
51. Risk Consciousness [26], [31]	52. Collaboration [16]
53. **Training Measures** [16], [28], [38], [47], [48], [29]	54. Security Culture [17], [22]
55. Technical Equipment (Quality) [18], [31], [47]	56. Technical Security Controls [17]
57. Tools [8], [28], [36]	58. Behavioural Controls [17]
59. Certification as Proof [25]	60. Maturity Models [50]

4.3 Integration of Requirements from Literature Review 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 provided 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 the requirements from the literature research. Table 4 provides an overview of the requirements (Table 4) from the NIS-2 Directive and the literature review.

Table 4. 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

5 From Requirements to a Procedural Model

In this section, the identified requirements are used as the basis for defining a procedural model that can help to introduce ISMSs in SPSO.

5.1 Requirements Structured

The requirements have been organized as follows. At the top hierarchical level, the requirements from the area of compliance must be met for an ISMS to be established. This is only possible if there are appropriate financial conditions in the organization. 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 the heading Strategy. In the area of human requirements, the implementation of training measures is essential. This is followed by the largest block of requirements: 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 1 summarises the results of Sections 4.1 and 4.2.

Further it is considered, what the requirements of the NIS 2 Directive are, on the one hand, and what the obstacles are, on the other hand, and how these requirements can be implemented quickly and easily through a rough process model in small and medium-sized municipal administrations.

The factors highlighted in grey colour in Figure 1 receive specific attention in the procedural model presented. The result of the literature research was that it is precisely these points that represent success factors for the development of an ISMS.

In a further development step, these requirements for an ISMS were transferred into a procedural model [12] shown in Figure 2. The procedural model is supported by an appropriate software prototype depicted in Figure 3. The procedural model and the software support fulfil the requirements of an ISMS through 12 steps (Figure 2) and help to meet the requirements of the NIS-2 Guidelines.

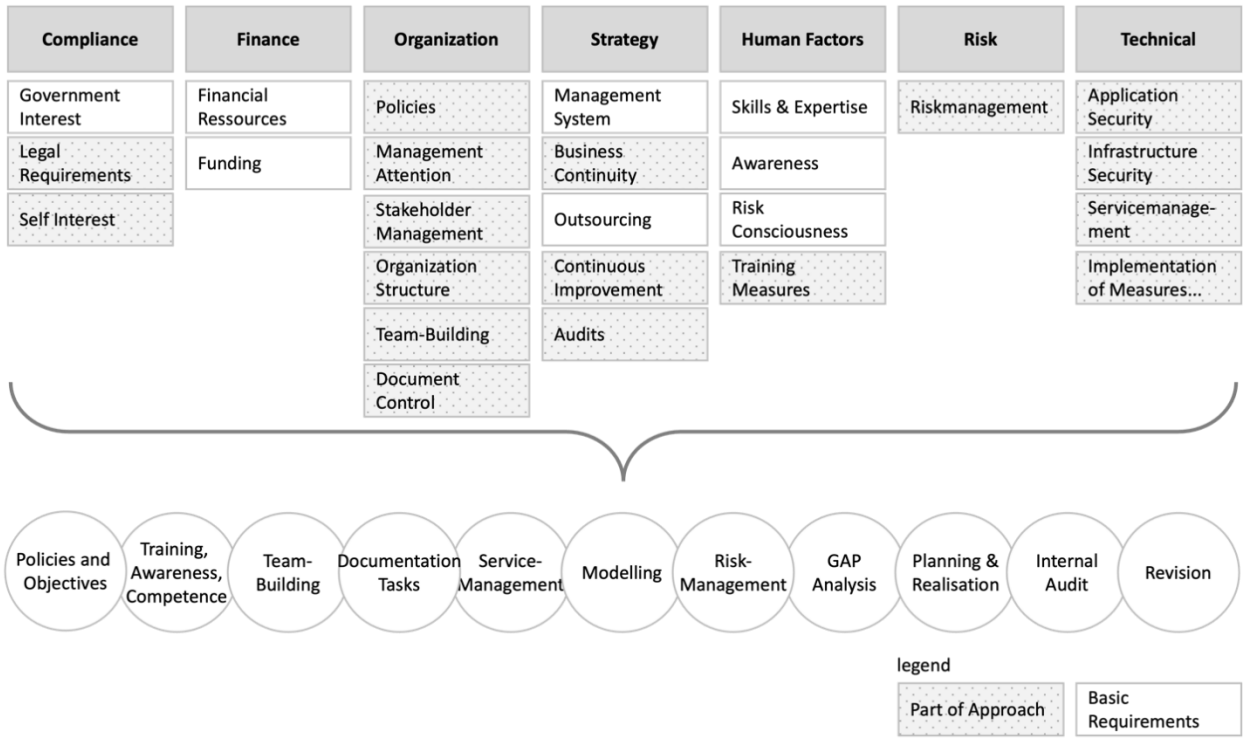

Figure 1. Structured Requirements for an ISMS as a foundation of the development of a Procedural Model

5.2 Initial Procedural Model

In essence, the procedural model explains five layers, 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 **building infrastructure layer** (perimeter) of the organization (Figure 2). The first two layers are strategic layers. The other three layers are to be understood as operational. It is precisely this distinction that distinguishes the presented model from other approaches, which often focus only on the operational layers [51, pp. 107–143].

A key point of the presented model is that compliance requirements are placed at the forefront of consideration. Especially in the area of public organizations, concrete tasks are derived from this [52, p. 187]. However, the same applies to small and medium-sized enterprises (SMEs). In the SME sector, for instance, compliance requirements include contractual and/or delivery terms and conditions as well as other compliances. To meet compliance requirements, processes are carried out in both types of organizations to fulfil the tasks associated with the contracts. It is precisely at this interface that the process model dovetails the strategic with the operational layer. 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) of GDPR.

Organizations that use the procedural model are supported along a given sequence of 12 steps in the development and establishment of 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 chief executive level (C-level). On the other hand, the ISMS that is to be established should also be founded by a policy. And also, in this step, it is necessary to develop a corresponding **target hierarchy**, taking into account the requirements and expectations of the stakeholders (interest groups).

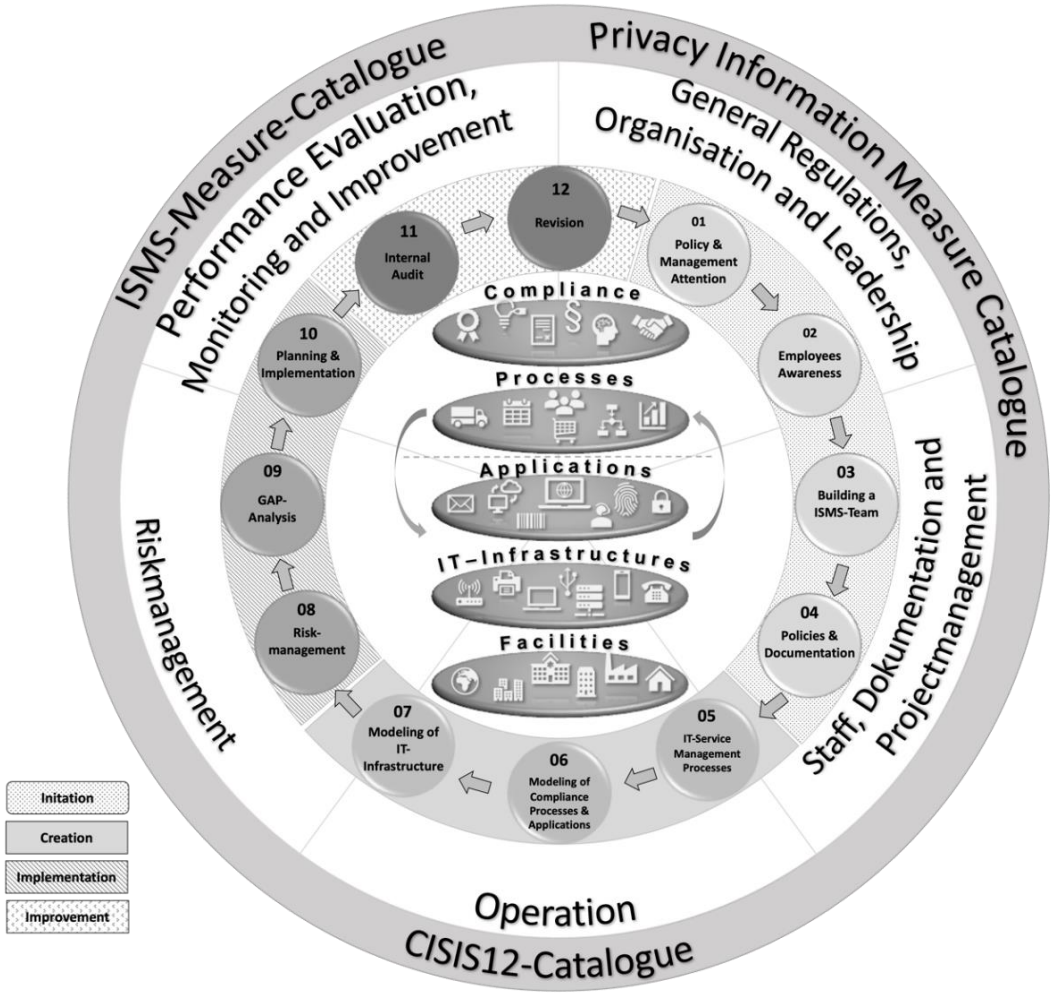

Figure 2. Initial solution architecture and procedural model

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 key 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 beginning (2nd step) of the procedural model.

The **team composition** is essential for the successful implementation of an ISMS. Depending on the size of the **organization**, it must be determined with which roles the upcoming ISMS project is to be carried out. It is essential 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 plan-do-check-act (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 the creation and updating of a **documentation structure** suitable for the ISMS. Documentation that is intended to support the organization in the operation of the ISMS, on the one hand, but also serves as proof of certification, on the other hand, must meet the requirements of structure, clarity, completeness, comprehensibility, correctness, traceability, objectivity, integrity, and authenticity. Traceability forms one of the foundations for the continuous improvement process (CIP) of the ISMS.

One of the main differences from other ISMS standards is the implementation of **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 processes**.

The new **legal requirements (compliances)** are often not sufficiently considered by management systems. These compliances are integrated into the procedural model through the first layer (Figure 2). 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 as 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 better assessing future events thus establishing a risk radar for both the strategic and operational view in the organization.

Following the risk assessment, the "assets – processes, applications, IT infrastructures and buildings" are evaluated with regard to the implementation of the measures from the selected security catalogues. This **target-actual** assessment should be carried out as part of a group dynamic process and represents a self-assessment. As a result, there is a **GAP-analysis** regarding the degree of implementation or maturity level of the ISMS already established. This process may be supported by external third parties.

The GAP-analysis is followed by the **planning and implementation** step. 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 even very elaborated ISMS potentially have room for improvement, which means that planning should always include the assessment if possible improvements actually are required and worth the investment. This also applies to the procedural model presented, because the degree of maturity of a management system only develops with several runs (clean in-place (CIP) process).

To measure this CIP process, an **internal audit** is planned in the next step of the presented solution architecture (Figure 2). With the help of an internal audit, the organization itself should be enabled to examine its own ISMS for weak points and to 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 the preparation of a management report. This management report is supplemented by documents such as the implementation plan and risk treatment plan and 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 layers (Compliance to Facilities) 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 be able 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 to other management systems (e.g., data protection with SDM 3.0, ISO 27001, CIS-Controls, BSI Compendium, KRITIS §8a, etc.).

The implementation steps from “01 Policy and Management Attention” to “12 Revision” depicted in the third (inner) ring of Figure 2 illustrate the core steps of the procedural model.

Figure 3 illustrates the basic idea of the envisioned software prototype: the status of all individual steps of the procedural model (01 to 12) and its different layers (Compliance to Facilities) has to be operational and visualized by metrics or indicators.

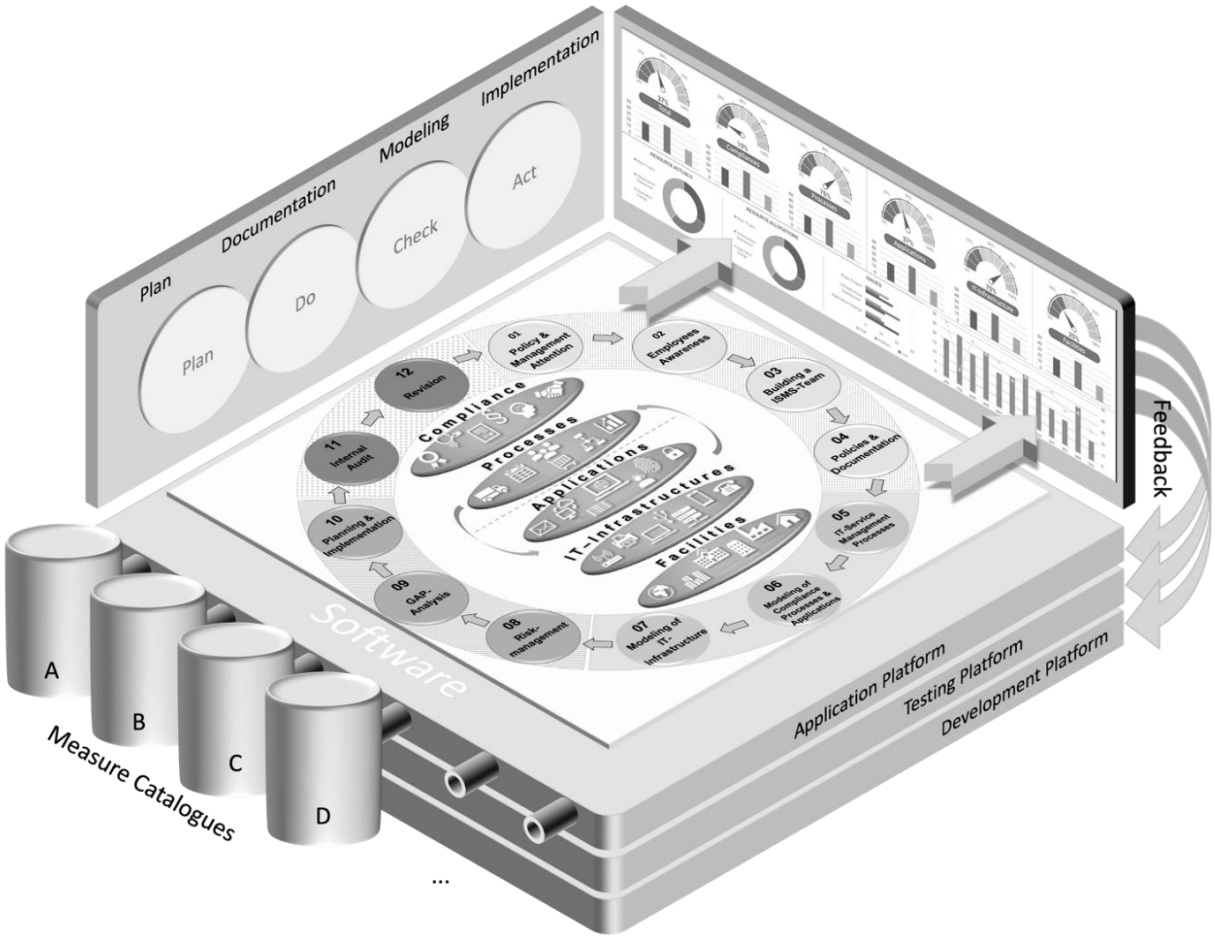

Figure 3. The Procedural Model integrated into a Software Prototype

The visualization is achieved by using dashboards. The procedural model and the layers are visible in the center of Figure 3, the dashboard is located in the top right and the overall monitoring process is shown in the top left (Plan, Do, Check, Act). In case such indicators already have been implemented in an organization, they can be taken from existing measure catalogues (bottom left). The software prototype as such consists of an application platform for operational use and a development and testing platform for preparing new features.

6 Summary, Future Work, and Limitation

The requirements of the NIS-2 Directive are a very abstract framework. Currently, there is a lack of corresponding architectural concepts [15, p. 824]. In combination with the architectural concept, an ISMS also must be established and operated sustainably. At the same time, the listed requirements from the NIS-2 Directive meet in practice the obstacles to the introduction of an ISMS.

Through a clear identification of the requirements of the NIS-2 Directive, but also of the obstacles described in Sections 4.1 and 4.2 and summarized in Figure 1, 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 discussed in this article must be considered in the development of 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 and the usability was checked in an artificial environment and a field test [12].

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 [53] are to be implemented with the help of the Framework for Evaluation Design Science (FEDS) [54].

However, a limitation must be taken into account, namely: 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 the introduction of 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 general be adapted to the needs but are too complex to be manageable for the municipalities. In principle, it is, for instance, possible 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 [55].

References

[1] M. Riek, R. Bohme, and T. Moore, “Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance,” *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 261–273, 2016. Available: https://doi.org/10.1109/TDSC.2015.2410795

[2] Raising Awareness of Cybersecurity, ENISA. Available: https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity. Accessed on Dec. 14, 2022.

[3] R. T. Watson and J. Webster, “Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0,” *Journal of Decision Systems*, vol. 29, no. 3, pp. 129–147, 2020. Available: https://doi.org/10.1080/12460125.2020.1798591

[4] F. Moses, K. Sandkuhl, and T. Kemmerich, “Information security management in German local government,” in *the 17th Conference on Computer Science and Intelligence Systems*, pp. 183–189, 2022. Available: https://doi.org/10.15439/2022F162

[5] 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), vol. 333. 2022 (in German). Available: http://data.europa.eu/eli/dir/2022/2555/oj/deu. Accessed on Jul. 10, 2023.

[6] P. Johannesson and E. Perjons, *An Introduction to Design Science*. Springer, 2014. Available: https://doi.org/10.1007/978-3-319-10632-8

[7] Bundesamt für Sicherheit in der Informationstechnik. Die Lage der IT-Sicherheit in Deutschland, 2023 (in German). Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html

[8] F. Moses, K. Sandkuhl, and T. Kemmerich, "Empirical Study on the State of Practice of Information Security Management in Local Government," in *Human Centred Intelligent Systems, Smart Innovation, Systems and Technologies*, Springer, vol. 310, pp. 13–25, 2022. Available: https://doi.org/10.1007/978-981-19-3455-1_2

[9] D. C. Leeser, *Digitalisierung in KMU kompakt: Compliance und IT-Security*. Springer, 2020 (in German). Available: https://doi.org/10.1007/978-3-662-59738-5

[10] N. Pohlmann, "Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung," in *Digitalisierung im Spannungsfeld von Politik, Wirtschaft, Wissenschaft und Recht*, Springer, pp. 195–212, 2018 (in German). Available: https://doi.org/10.1007/978-3-662-56438-7_15

[11] I. Henseler-Unger and A. Hillebrand, "Aktuelle Lage der IT-Sicherheit in KMU: Wie kann man die Umsetzungslücke schließen?" *Datenschutz Datensicherheit DuD*, vol. 42, no. 11, pp. 686–690, 2018 (in German). Available: https://doi.org/10.1007/s11623-018-1025-y

[12] F. Moses and K. Sandkuhl, "Mit CISIS12 ein ISMS aufbauen," *Datenschutz Datensicherheit DuD*, vol. 46, no. 10, pp. 654–659, 2022 (in German). Available: https://doi.org/10.1007/s11623-022-1677-5.

[13] P. Weissmann, "Die neue EU NIS 2 Direktive für Cyber Security in KRITIS" (in German). Available: https://www.openkritis.de/it-sicherheitsgesetz/eu-nis-2-direktive-kritis.html. Accessed on May 09, 2023.

[14] P. Eckhardt and A. Kotovskaia, "The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive," *Int. Cybersecur. Law Rev.*, vol. 4, no. 2, pp. 147–164, 2023. Available: https://doi.org/10.1365/s43439-023-00084-z

[15] C. Werner, N. Brinker, and O. Raabe, "Grundlagen für ein gesetzliches IT-Sicherheitsrisikomanagement – Ansätze zur Vereinheitlichung von Rollenmodell, Risikomanagement und Definitionen für das IT-Sicherheitsrecht," *Computer und Recht*, vol. 38, no. 12, pp. 817–824, 2022 (in German). Available: https://doi.org/10.9785/cr-2022-381219.

[16] P. Choejey, D. Murray, and C. Che Fung, "Exploring Critical Success Factors for Cybersecurity in Bhutan's Government Organizations," in *Computer Science & Information Technology (CS & IT)*, Academy & Industry Research Collaboration Center (AIRCC), pp. 49–61, 2016. Available: https://doi.org/10.5121/csit.2016.61505

[17] H. W. Glaspie and W. Karwowski, "Human Factors in Information Security Culture: A Literature Review," in *Advances in Human Factors in Cybersecurity*, *Advances in Intelligent Systems and Computing*, Springer, vol. 593, pp. 269–280, 2018. Available: https://doi.org/10.1007/978-3-319-60585-2_25

[18] E. B. S. Çubuk, H. E. Zeren, and B. Demirdöven, "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, 2022. Available: https://doi.org/10.4018/978-1-6684-5284-4.ch020

[19] T. Rehbohm, K. Sandkuhl, C. H. Cap, and T. Kemmerich, "Integrated Security Management of Public and Private Sector for Critical Infrastructures – Problem Investigation," in *Business Information Systems Workshops, Lecture Notes in Business Information Processing*, Springer, vol. 444, pp. 291–303, 2022. Available: https://doi.org/10.1007/978-3-031-04216-4_26

[20] M. Taddeo, "Is Cybersecurity a Public Good?" *Minds & Machines*, vol. 29, no. 3, pp. 349–354, 2019. Available: https://doi.org/10.1007/s11023-019-09507-5

[21] S. Nather, "Improving Information Security Through Risk Management and Enterprise Architecture Integration," in *International Conference on Cyber Warfare and Security*, Academic Conferences International Limited, 2018, p. 420.

[22] L. Khansa, J. Kuem, M. Siponen, and S. S. Kim, "To Cyberloaf or Not to Cyberloaf: The Impact of the Announcement of Formal Organizational Controls," *Journal of Management Information Systems*, vol. 34, no. 1, pp. 141–176, 2017, Available: https://doi.org/10.1080/07421222.2017.1297173

[23] V. Susukailo, I. Opirsky, and O. Yaremko, “Methodology of ISMS Establishment Against Modern Cybersecurity Threats,” in *Future Intent-Based Networking, Lecture Notes in Electrical Engineering*, Springer, vol. 831, pp. 257–271, 2022. Available: https://doi.org/10.1007/978-3-030-92435-5_15

[24] N. Poehlmann, K. M. Caramancion, I. Tatar, Y. Li, M. Barati, and T. Merz, “The Organizational Cybersecurity Success Factors: An Exhaustive Literature Review,” in *Advances in Security, Networks, and Internet of Things, Transactions on Computational Science and Computational Intelligence*, Springer, pp. 377–395, 2021. Available: https://doi.org/10.1007/978-3-030-71017-0_27

[25] B. Preis and L. Susskind, “Municipal Cybersecurity: More Work Needs to be Done,” *Urban Affairs Review*, vol. 58, no. 2, pp. 614–629, 2022. Available: https://doi.org/10.1177/1078087420973760

[26] K. Gedris *et al.*, “Simulating municipal cybersecurity incidents: Recommendations from expert interviews,” in *the Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 2036–2045, 2021. Available: https://doi.org/10.24251/HICSS.2021.249

[27] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, “Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry,” *Sustainability*, vol. 14, no. 3, Article 1269, 2022. Available: https://doi.org/10.3390/su14031269

[28] I. Nikolova, “Best Practice for Cybersecurity Capacity Building in Bulgaria’s Public Sector,” *ISIJ*, vol. 38, pp. 79–92, 2017. Available: https://doi.org/10.11610/isij.3806

[29] T. van Steen and J. R. A. Deeleman, “Successful Gamification of Cybersecurity Training,” *Cyberpsychology, Behavior, and Social Networking*, vol. 24, no. 9, pp. 593–598, 2021. Available: https://doi.org/10.1089/cyber.2020.0526

[30] E. Koza, “Eine empirische Kontentanalyse zur Ermittlung von praxisorientierten Optimierungsfeldern zur Resilienz-Erhöhung der IT-Systeme im Sinne der ganzheitlichen Betrachtung der Informationssicherheit,” in *INFORMATIK 2021, Workshop: Security, Datenschutz und Anonymisierung*, Gesellschaft für Informatik, 2021 (in German). Available: https://doi.org/10.18420/informatik2021-070

[31] A. Chodakowska, S. Kańduła, and J. Przybylska, “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, 2022. Available: https://doi.org/10.4335/20.1.161-192(2022)

[32] V. Benson, J. McAlaney, and L. A. Frumkin, “Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape,” *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications*, pp. 1264–1269, 2019. Available: https://doi.org/10.4018/978-1-5225-8897-9.ch062

[33] K. Arbanas and N. Žajdela Hrustek, “Key Success Factors of Information Systems Security,” *Journal of Information and Organizational Sciences*, vol. 43, no. 2, pp. 131–144, 2019. Available: https://doi.org/10.31341/jios.43.2.1

[34] J. Forrester, M. L. Lopez, and M. D. Valentina, “Marketing a cybersecurity Awareness Solution in LPA Contexts,” in *Cybersecurity Awareness, Advances in Information Security*, Springer, vol. 88, pp. 161–181, 2022. Available: https://doi.org/10.1007/978-3-031-04227-0_7

[35] J. H. Awan, “Security strategies to overcome cyber measures, factors and barriers,” *Engineering Science and Technology International Research Journal*, vol. 1, no. 1, 2017.

[36] S. B. M. Sabtu and K. M. Mohamad, “Critical Information Infrastructure Protection Requirement for the Malaysian Public Sector,” in *Advances on Smart and Soft Computing, Advances in Intelligent Systems and Computing*, Springer, vol. 1188, pp. 371–381, 2021. Available: https://doi.org/10.1007/978-981-15-6048-4_32

[37] R. Tatiara, A. N. Fajar, B. Siregar, and W. Gunawan, “Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001,” *J. Phys.: Conf. Ser.*, vol. 978, no. 1, p. 012039, 2018. Available: https://doi.org/10.1088/1742-6596/978/1/012039

[38] P. Cooke, ““Digital tech” and the public sector: what new role after public funding?” *European Planning Studies*, vol. 25, no. 5, pp. 739–754, 2017. Available: https://doi.org/10.1080/09654313.2017.1282067

[39] K. Zheng, L. A. Albert, J. R. Luedtke, and E. Towle, “A budgeted maximum multiple coverage model for cybersecurity planning and management,” *IISE Transactions*, vol. 51, no. 12, pp. 1303–1317, 2019. Available: https://doi.org/10.1080/24725854.2019.1584832

[40] K. M. N. De Abrew and R. Wickramarachchi, “Organizational Factors Affecting the ISMS Effectiveness in Sri Lankan IT Organizations: A Systematic Review,” in *Proceedings of the International Conference on Industrial Engineering and Operations Management*, pp. 702–713, 2021.

[41] M. S. Jalali, B. Russell, S. Razak, and W. J. Gordon, "EARS to cyber incidents in health care," *Journal of the American Medical Informatics Association*, vol. 26, no. 1, pp. 81–90, 2019. Available: https://doi.org/10.1093/jamia/ocy148

[42] B. Farrand and H. Carrapico, "Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity," *European Security*, vol. 31, no. 3, pp. 435–453, 2022, Available: https://doi.org/10.1080/09662839.2022.2102896

[43] A. Sengupta, "A Stakeholder-Centric Approach for Defining Metrics for Information Security Management Systems," in *Risks and Security of Internet and Systems, Lecture Notes in Computer Science*, Springer, vol. 13204, pp. 57–73, 2022. Available: https://doi.org/10.1007/978-3-031-02067-4_4

[44] S. P. Chainey and A. Alonso Berbotto, "A structured methodical process for populating a crime script of organized crime activity using OSINT," *Trends Organ Crim*, vol. 25, no. 3, pp. 272–300, 2022, Available: https://doi.org/10.1007/s12117-021-09428-9

[45] D. O. Potter and J. S. Hurley, "The new role of the "Next generation" CFO," in *the Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*, pp. 398–401, 2020. Available: https://doi.org/10.34190/ICCWS.20.096

[46] H. Hui-Lin and W. Kuei-Min, "The critical success factors assessment of ISO 27001 certification in computer organization by test-retest reliability," *Afr. J. Bus. Manage.*, vol. 8, no. 17, pp. 705–716, 2014. Available: https://doi.org/10.5897/AJBM2014.7443

[47] F. Alkhudhayr, S. Alfarraj, B. Aljameeli, and S. Elkhdiri, "Information Security: A Review of Information Security Issues and Techniques," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1–6, 2019. Available: https://doi.org/10.1109/CAIS.2019.8769504

[48] S. Schmitz-Berndt and P. G. Chiara, "One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive," *Int. Cybersecur. Law Rev.*, vol. 3, no. 2, pp. 289–311, 2022. Available: https://doi.org/10.1365/s43439-022-00058-7

[49] J. Kävrestad, S. Furnell, and M. Nohlberg, "What Parts of Usable Security Are Most Important to Users?" in *Information Security Education for Cyber Resilience*, *IFIP Advances in Information and Communication Technology*, Springer, vol. 615, pp. 126–139, 2021. Available: https://doi.org/10.1007/978-3-030-80865-5_9

[50] H. J. Clemith and D. C. Sicker, "Maturity and Process Capability Models and Their Use in Measuring Resilience in Critical Infrastructure Protection Sectors," *IJSITA*, vol. 5, no. 2, pp. 44–63, 2014. Available: https://doi.org/10.4018/ijsita.2014040104

[51] T. Liedtke, *Informationssicherheit: Möglichkeiten und Grenzen*. Springer, 2022 (in German). Available: https://doi.org/10.1007/978-3-662-63917-7

[52] L. Bostelmann, "Cybersicherheit bei der Umsetzung des Onlinezugangsgesetzes – Digitalisierung ja, aber (rechts)sicher!" in *Handbuch Onlinezugangsgesetz: Potenziale – Synergien – Herausforderungen*, Springer, pp. 165–197, 2021 (in German). Available: https://doi.org/10.1007/978-3-662-62395-4_8

[53] A. Hevner and S. Chatterjee, "Design Science Research in Information Systems," in *Design Research in Information Systems: Theory and Practice*, Springer, vol. 22, pp. 9–22, 2010. Available: https://doi.org/10.1007/978-1-4419-5653-8_2

[54] J. Venable, J. Pries-Heje, and R. Baskerville, "FEDS: a Framework for Evaluation in Design Science Research," *Eur J Inf Syst*, vol. 25, no. 1, pp. 77–89, 2016. Available: https://doi.org/10.1057/ejis.2014.36

[55] R. Alm and M. Wißotzki, "TOGAF Adaption for Small and Medium Enterprises," in *Business Information Systems Workshops*, *Lecture Notes in Business Information Processing*, Springer, vol. 160, pp. 112–123, 2013. Available: https://doi.org/10.1007/978-3-642-41687-3_12