ISMS in small public sector organisations: requirements and design of a procedural approach

Frank Moses[1], Kurt Sandkuhl[1]

[1] *University of Rostock, Albert-Einstein-Str. 22, 18059 Rostock, Germany*

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 important aspects of most public sector organisations. The dependency on technology for almost every single process in an organisation has put ISMS at the top of the corporate agenda of public sector organisations. For public organisations 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 paper 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 organisations (SPSO). At the same time, minimum requirements should be defined that help municipal administration set up an information security management system quickly and easily. This paper summarizes the different requirements and generates a foundation for a rough procedural model, for implementing the upcoming requirements of the NIS 2 Directive quickly and easily in local governments.

Keywords

Hindering Factors, Requirements, Information Security, ISMS [1]

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. 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 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 the public sector [2, p. 710], [3, 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 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 organisation. 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 experience after 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

BIR-WS 2023: BIR 2023 Workshops and Doctoral Consortium, 22nd International Conference on Perspectives in Business Informatics Research (BIR 2023), September 13-15, 2023, Ascoli Piceno, Italy

frank.moses@uni-rostock.de (F. Moses); kurt.sandkuhl@uni-rostock.de (K. Sandkuhl)

0009-0008-8117-7233 (F. Moses); 0000-0002-7431-8412 (K. Sandkuhl)

approach tailored to their demands. The current requirements of the NIS-2 Directive [5]should be considered.

Chapter "2 Methodology" describes the phases of the Design Science approach, which are progressed through step by step. Chapter "3 Identifying the requirements for an adoption and diffusion of an ISMS" is divided into 3 subsections. First, the identification of 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 in a further step in order to develop and describe a rough process model based on them. In the fourth chapter, a rough process model is derived from the requirements and described. 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.

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

Table 1.
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	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 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. Identifying the requirements for an adoption and diffusion of an isms

3.1. 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:[7]

- **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.[8] In Art. 21 of the NIS-2 Directive, four **core requirements** are formulated that must be met by an ISMS.[7] 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.[9, p. 824]

3.2. The requirements from literature research

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. Behind each hindering factor, the reference is listed in brackets [citation] (Table 3). On the one hand, this summary serves as the basis of this paper in the sense of Design Science Research (DSR) an overview of the disruptive factors of an ISMS. But also, at the same time as a foundation for further research work. The determined requirements that are important for this paper are marked in **bold** in Table 3.

Table 3:
Identified Hindering Factors resp. Critical Success Factors

Factor / Requirement	Factor / Requirement
1. **Change management** [10]	2. Incentives (Tariff Structure) [11]
3. Application Security [12]	4. Cybersecurity Architecture [13], [14], [15]
5. Audits [10], [11], [16], [17]	6. ISMS-Organization [10], [18]
7. **Risk Management** [19], [17], [20]–[22], [18], [15]	8. **Education Level of Employees** [11], [23], [24], [21], [25]
9. **Awareness of Employees** [10], [11], [26], [27], [28]	10. Size of the Agency[29]

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

3.3. Merge 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 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 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

4. From requirements to a first approach of a procedural model

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 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, training measures are essential to be implemented. 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 from Sections 3.1 and 3.2.

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?

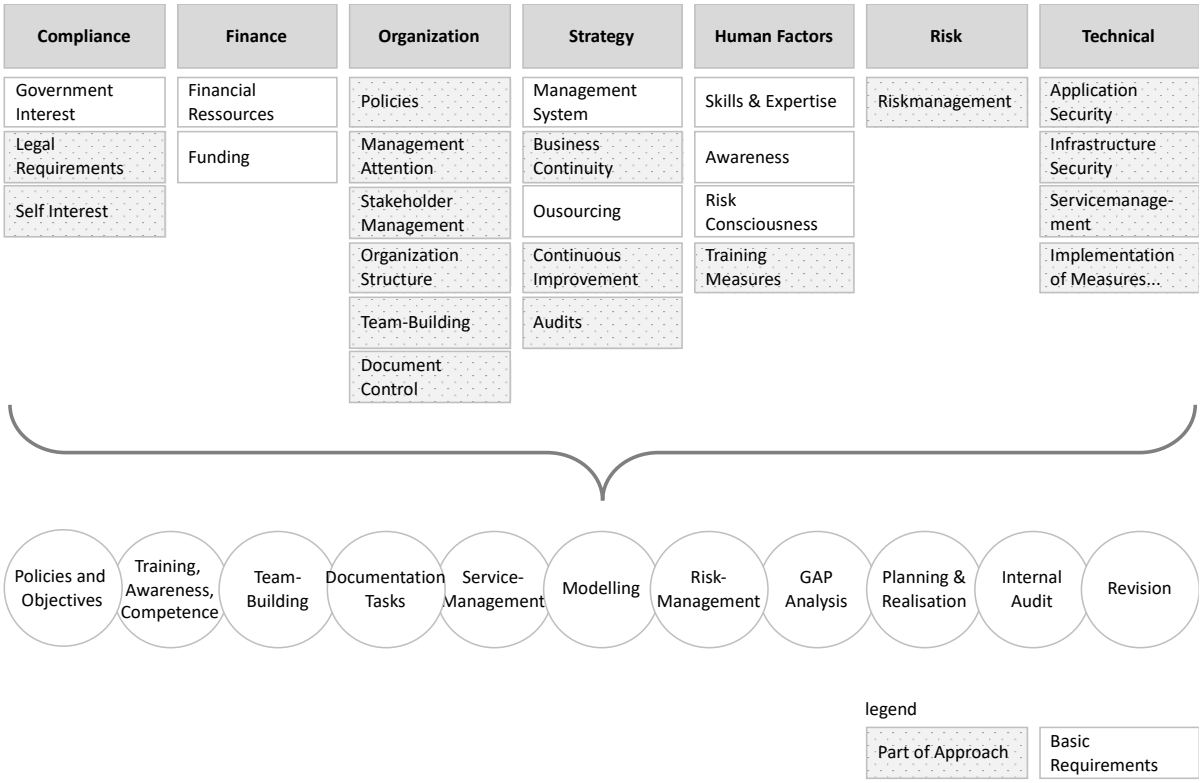

Figure 1: Structured Requirements for an ISMS as a foundation of the development of a Procedural Model

In a further development step, these requirements for an ISMS were transferred into a procedural model. The procedural model is supported by an appropriate software prototype. The procedural model and the software support (**Figure 2**) with the help of 12 steps the requirements of an ISMS and help fulfill the requirements of the NIS-2-Directive.

5. Summary and next steps

The requirements of the NIS-2 Directive are very abstract framework. Currently, there is a lack of corresponding architectural concepts.[9, p. 824] Below this architecture, an ISMS 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 from Sections 3.1 and 3.2 an 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 listed above 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 (Figure 2) and the usability was checked in an artificial environment and in the field test [48]. 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 [49] are to be implemented with the help of the Framework for Evaluation Design Science (FEDS) [50].

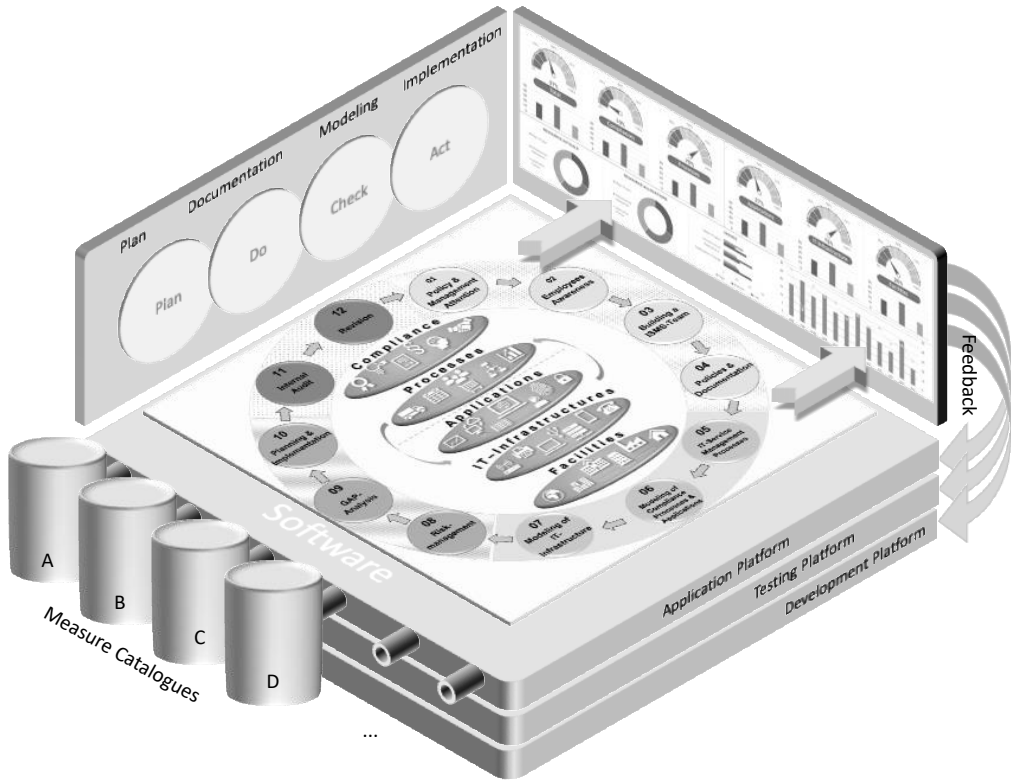

Figure 2: The Procedural Model integrated into a Software Prototype

References

[1] M. Riek, R. Bohme, and T. Moore, 'Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance', *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 2.

[2] 'Raising Awareness of Cybersecurity', *ENISA*, 2022. https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity (accessed 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', *J. Decis. Syst.*, vol. 29, no. 3, pp. 129–147, Jul. 2020.

[4] F. Moses, K. Sandkuhl, and T. Kemmerich, 'Information security management in German local government', presented at the 17th Conference on Computer Science and Intelligence, 2022.

[5] *Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates 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.

[6] P. Johannesson and E. Perjons, *An Introduction to Design Science*.

[7] P. Weissmann, 'Die neue EU NIS 2 Direktive für Cyber Security in KRITIS', 2023. https://www.openkritis.de/it-sicherheitsgesetz/eu-nis-2-direktive-kritis.html.

[8] P. Eckhardt and A. Kotovskaia, 'The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive', *Int. Cybersecurity Law Rev.*, vol. 4, no. 2, 2023.

[9] C. Werner, N. Brinker, and O. Raabe, 'Grundlagen für ein gesetzliches IT-Sicherheitsrisikomanagement — Ansätze zur Vereinheitlichung von Rollenmodellen, Risikomanagement für das IT-Sicherheitsrecht', *Comput. Recht*, vol. 38, 2023.

[10] 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), Dec. 2016, pp. 49–61.

[11] H. W. Glaspie and W. Karwowski, 'Human Factors in Information Security Culture: A Literature Review', in *Advances in Human Factors in Cybersecurity*, D. Nicholson, Ed., in Advances in Intelligent Systems and Computing.

[12] 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, 2022.
[13] 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*, W. Abramowicz, S. Auer, and M. Stróżyna, Eds., 2022.
[14] M. Taddeo, 'Is Cybersecurity a Public Good?', *Minds Mach.*, vol. 29, no. 3, pp. 349–354.
[15] S. Nather, 'Improving Information Security Through Risk Management and Enterprise Architecture Integration', in *International Conference on Cyber Warfare and Security*, Academic Conferences International Limited, Jan. 2018, p. 420.
[16] 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', *J. Manag. Inf. Syst.*, vol. 34, no. 1.
[17] V. Susukailo, I. Opirsky, and O. Yaremko, 'Methodology of ISMS Establishment Against Modern Cybersecurity Threats', in *Future Intent-Based Networking*, M. Klymash, M. Beshley, and A. Luntovskyy, Eds., in Lecture Notes in Electrical Engineering.
[18] 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*, K. Daimi, H. R. Arabnia, L. Deligiannidis, M.-S. Hwang, and F. G. Tinetti, Eds., in Transactions on Computational Science and Computational Intelligence.
[19] B. Preis and L. Susskind, 'Municipal Cybersecurity: More Work Needs to be Done', *Urban Aff. Rev.*, vol. 58, no. 2, pp. 614–629, Mar. 2022, doi: 10.1177/1078087420973760.
[20] 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*, A. Zimmermann, R. J. Howlett, and L. C. Jain, Eds., in Smart Innovation, Systems and Technologies. Singapore: Springer Nature, 2022, pp. 13–25.
[21] K. Gedris *et al.*, 'Simulating municipal cybersecurity incidents: Recommendations from expert interviews', presented at the Proceedings of the Annual Hawaii International Conference on System Sciences, 2021, pp. 2036–2045.
[22] 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, Art. no. 3, Jan. 2022.
[23] I. Nikolova, 'Best Practice for Cybersecurity Capacity Building in Bulgaria's Public Sector', *Inf. Secur. Int. J.*, vol. 38, pp. 79–92, 2017, doi: 10.11610/isij.3806.
[24] T. van Steen and J. R. A. Deeleman, 'Successful Gamification of Cybersecurity Training', *Cyberpsychology Behav. Soc. Netw.*, vol. 24, no. 9, pp. 593–598, Sep. 2021.
[25] E. Koza, *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, 2021.
[26] A. CHODAKOWSKA, S. KAŃDUŁA, and J. PRZYBYLSKA, 'Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done', *Lex Localis - J. Local Self-Gov.*, vol. Vol. 20, No. 1, Jan. 2022.
[27] V. Benson, J. McAlaney, and L. A. Frumkin, 'Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape', *Cyber Law Priv. Secur. Concepts Methodol. Tools Appl.*, pp. 1264–1269, 2019, doi: 10.4018/978-1-5225-8897-9.ch062.
[28] K. Arbanas and N. Žajdela Hrustek, 'Key Success Factors of Information Systems Security', *J. Inf. Organ. Sci.*, vol. 43, no. 2, pp. 131–144, Dec. 2019, doi: 10.31341/jios.43.2.1.
[29] J. Forrester, M. L. Lopez, and M. D. Valentina, 'Marketing a cybersecurity Awareness Solution in LPA Contexts', in *Cybersecurity Awareness*, J. Andriessen, T. Schaberreiter, A. Papanikolaou, and J. Röning, Eds., in Advances in Information Security.
[30] J. H. Awan, 'Security strategies to overcome cyber measures, factors and barriers', *Eng. Sci. Technol. Int. Res. J.*, vol. Vol.1, No. 1, Apr. 2017.
[31] 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*, F. Saeed, T. Al-Hadhrami, F. Mohammed, and E. Mohammed, Eds., in Advances in Intelligent

Systems and Computing. Singapore: Springer, 2021, pp. 371–381.
[32] 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, Mar. 2018.
[33] P. Cooke, '"Digital tech" and the public sector: what new role after public funding?', *Eur. Plan. Stud.*, vol. 25, no. 5, pp. 739–754, May 2017, doi: 10.1080/09654313.2017.1282067.
[34] K. Zheng, L. A. Albert, J. R. Luedtke, and E. Towle, 'A budgeted maximum multiple coverage model for cybersecurity planning and management', *IISE Trans.*, vol. 51, no. 12.
[35] K. M. N. De Abrew and R. Wickramarachchi, 'Organizational Factors Affecting the ISMS Effectiveness in Sri Lankan IT Organizations: A Systematic Review', 2021.
[36] E. Koza, *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, 2021.
[37] M. S. Jalali, B. Russell, S. Razak, and W. J. Gordon, 'EARS to cyber incidents in health care', *J. Am. Med. Inform. Assoc.*, vol. 26, no. 1, pp. 81–90, Jan. 2019, doi: 10.1093/jamia/ocy148.
[38] B. Farrand and H. Carrapico, 'Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity', *Eur. Secur.*, vol. 31, no. 3, 2022.
[39] F. Moses, K. Sandkuhl, and T. Kemmerich, 'Empirical Study on the State of Practice of Information Securty Maturity Management in Local Government.', in *Human Centred Intelligent Systems 2022 - Proceeding of the 15th International Conference on Human Centred Intelligent Systems (KES-HCIS-22). Smart Innovation, Systems and Technologies.*, A. Zimmermann, Ed., Springer. Accepted for publication. To appear June 2022., 2022.
[40] A. Sengupta, 'A Stakeholder-Centric Approach for Defining Metrics for Information Security Management Systems', in *Risks and Security of Internet and Systems*, B. Luo, M. Mosbah, F. Cuppens, L. Ben Othmane, N. Cuppens, and S. Kallel, Eds., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2022, pp. 57–73.
[41] S. P. Chainey and A. Alonso Berbotto, 'A structured methodical process for populating a crime script of organized crime activity using OSINT', *Trends Organ. Crime*, vol. 25, no. 3, pp. 272–300, Sep. 2022.
[42] D. O. Potter and J. S. Hurley, 'The new role of the "Next generation" CFO', presented at the Proceedings of the 15th International Conference on Cyber Warfare and Security, 2022.
[43] 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. Manag.*, vol. 8, no. 17, pp. 705–716, Sep. 2014.
[44] 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)*, May 2019, pp. 1–6.
[45] 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. Cybersecurity Law Rev.*, vol. 3, no. 2, pp. 289–311, Dec. 2022.
[46] J. Kävrestad, S. Furnell, and M. Nohlberg, 'What Parts of Usable Security Are Most Important to Users?', in *Information Security Education for Cyber Resilience*, L. Drevin, N. Miloslavskaya, W. S. Leung, and S. von Solms, Eds., in IFIP Advances in Information and Communication Technology. Cham: Springer International Publishing, 2021, pp. 126–139.
[47] H. J. Clemith and D. C. Sicker, 'Maturity and Process Capability Models and Their Use in Measuring Resilience in Critical Infrastructure Protection Sectors', *Int. J. Strateg. Inf. Technol. Appl. IJSITA*, vol. 5, no. 2, pp. 44–63, Apr. 2014.
[48] F. Moses and K. Sandkuhl, 'Mit CISIS12 ein ISMS aufbauen', *Datenschutz Datensicherheit .*
[49] A. Hevner and S. Chatterjee, 'Design Science Research in Information Systems', in *Design Research in Information Systems: Theory and Practice*, A. Hevner and S. Chatterjee, Eds., in Integrated Series in Information Systems. Boston, MA: Springer US, 2010, pp. 9–22.
[50] 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, Jan. 2016.