24th International Conference on Business Information Systems (BIS 2021)

Social Media

https://doi.org/10.52825/bis.v1i.43

Published: 02 July 2021

Development of the Information Security Management System Standard for Public Sector Organisations in Estonia

Mari Seeba[1, 2, [0000-0002-9066-2467]], Raimundas Matulevičius[1, [0000-0002-1829-4794]], and Ilmar Toom[2]

[1] Institute of Computer Science, University Of Tartu, Estonia

[2]Estonian Information System Authority, Tallinn Estonia

Abstract. Standardisation gives us a common understanding or processes to do something in a commonly accepted way. In information security management, it means to achieve the appropriate security level in the context of known and unknown risks. Each government's goal should be to provide digital services to its citizens with the acceptable level of confidentiality, integrity and availability. This study elicits the EU countries' requirements for information security management system (ISMS) standards and provides the standards' comparison requirements. The Estonian case is an example to illustrate the method when choosing or developing the appropriate ISMS standard to public sector organisations.

Keywords: Information Security Management System, ISMS, Public Sector, Requirements of Security Standards, Estonia

Introduction

Standardisation aims to optimise the process management, compare defined objects with each other, enable integration and interoperability of systems, cost optimisation and preparedness to adapt to new situations [1]. There are standards designed for information security management systems (ISMS) as well (few examples are [20, 21, 22]). In private organisation the management decides which ISMS standard to follow based on organisation requirements. At the national level the stakeholders' objectives and the national characteristics (e.g. unique technologies such as the X-tee [2] or electronic identity solutions [3]), and cultural and linguistic peculiarities should be considered independently of each organisation requirements. There is also a need for the standard long-term central maintenance and reduction of administrative costs, or compliance with the regulations (e.g. EU GDPR [5]). At the national level the ISMS standard must ensure a comprehensive national defence and systems interoperability carried out by each organisation. EU regulation (NIS Directive [6]) defines the cross-union incident management and information sharing rules, but it does not provide the information security management framework for public sector organisations.

There is no standardised method or requirements on how to compare and show different approaches of the ISMS standards for public sector organisations at the national level. This method should consider the standards substantive comparison, the national security strategic objectives, and external interested parties' requirements or abilities. On the national strategic level this method can support decision makers, and also security specialists to find relevant arguments when choosing or planning to create an ISMS standard. This study aims to investigate *what are the requirements to develop information security management standards for public sector organisations at the national level.*

The paper is motivated by the development of the national ISMS standard for the Estonian public sector organisations. In this study we identify and structure the requirements for national ISMS using 12 EU national cybersecurity strategies. Then we share the example of how Estonian ISMS requirements can be structured using our study approach. Using the elicited requirements we compare three ISMS standards and illustrate how the assessment of the ISMS standards with the elicited requirements can be done based on the Estonian case. Our experience shows that the comparison of the elicited and sorted requirements and ISMS standards is a possible way that can be followed by the other countries that are looking for ISMS standards or framework for public sector organisations.

The paper is structured as follows: Sect. 1 gives an overview of the Estonian case and related work. Sect. 2 describes the research method. Sect. 3.1 guides the ISMS standards requirements elicitation and structuring and Sect. 3.2 illustrates the use of requirements in comparison of standards and presents the results with the Estonian case. Finally, Sect. 4 concludes the paper with the results and limitations.

1 Background

1.1 Case Description

Estonia is an EU country with 1.33 million inhabitants. Estonia is known for its digital society imago and with the successful response to the first large-scale cyberattack against the entire state [15]. Estonian citizens, e-residents and organisations can use or provide more than 2860 digital services via eGovernment supported Data Exchange Layer X-tee (Estonian instance of the X-Road). More than 150 million requests per month are made via X-tee [16]. Majority of the transactions are made between public sector organisations. This context requires a clear understanding and mutual recognition of information security from the data exchange partners and data processors. The Estonian first version of information security management baseline standard called ISKE was developed and published in 2004 [27]. Now Estonia is developing its new national ISMS standard. In this paper we use Estonian case to illustrate how the elicited requirements for national ISMS can be used.

1.2 Related Works

We investigated the studies dealing with requirements to the ISMS standards and standards comparison.
European Union Agency for Cybersecurity (ENISA) certification standards review report [12] is indispensable to understand the origin and functioning of standardisation organisations. The report is focused on certification, and provides assessment guidance on the certification schemes, but it does not provide direct input to the comparison of standards.

EU SPARTA project includes the overview of the security-related certification initiatives and the related standards at the national and international level, as one of it’s deliverable [10]. It’s aim is to inform project partners about available standards that the project partners can consider certifying their project deliverable against. The report does not follow any exact requirement or comparison requirement.

Pertinent collection of security standards are systematised by standardisation bodies authority, jurisdiction, applicability, document type and standards examples in [8]. This overview did not describe the requirements to follow or which characteristics of the standards to compare.

Overviews and summaries of standards can be found from security blogs or websites of the consulting companies. A similar descriptive approach can be found in [9]. The paper covers ISO security-related standards and mentions the Information Security Forum (ISF) Standard of Good Practice for Information Security, COBIT (ISACA framework) and BSI IT-Grundschutz (IT baseline protection). This work only describes the standards, not focusing on the requirements or comparison.

A systematic approach to the content analysis of the standards can be found in [7], where the authors have created the conceptual model for security standards and provide the template for the standards content comparison. Their approach can help organisations, but do not help at the national strategic level.

By standards web-sites, the content comparison is provided for standards compliance confirmation. Usually, there are tables where each row represents similar control of comparable standards [24, 28]. These comparisons provide the sentence-by-sentence compliance confirmation on standard contents, but do not deal with other properties of the standard.

Finnish report [11] compares the cybersecurity situation of eight countries on the state level. The report provides a comparison of economical, educational, legal and social aspects of cybersecurity, and names the approaches of these eight countries. The report helped us to consider the relevant areas of the countries cybersecurity strategies.

The Estonian case can be illustrated with studies conducted in 1998 and 2003, which analysed the national security needs and security specialists ability to manage ISMS standards. The studies concluded, that Estonia needs baseline security with granular security measures catalog. [4] The same statements apply in today’s Estonia [19]. ENISA report [13] compares 28 EU state cybersecurity strategies and has identified that one common strategic objective is to establish baseline security measures to harmonize the security practices in the public and private sector. Report did not create requirements for that.

Related works showed several approaches on how to compare the security standards and gave some overview of the standards. The related works did not give any suggestions or requirements on how to choose ISMS standards for public sector organisations on the national strategic level. Also, we revealed that national cybersecurity strategies could be an appropriate source of requirements elicitation for ISMS standards.

2 Research Approach

The research demonstrates the requirements elicitation when developing the ISMS standard, illustrated using the Estonian case presented in Sect.1.1. The paper’s goal is to answer the question **RQ:** *what are the requirements to develop information security management standards for public sector organisations on the national level?* The research question can be divided into two subquestions: **RQ1:** how to find and what are the countries requirements to the ISMS standard? **RQ2:** how to use these requirements when developing the national ISMS standard?

Our research process is case-oriented and is illustrated in Fig. 1. We conducted two parallel processes. Firstly, theoretical approach is used to elicit requirements for ISMS standard (activity 1.1) at the national level. It is based on the National Cybersecurity Index (NCSI) [14] database (input 1.1.a) to answer RQ1. The structured result of ISMS standard requirements (artefact 1.1.b) were used to elicit the Estonian ISMS standard requirements (activity 2.1 and artifact 2.1.a). Secondly, activity 1.2 uses the output of 1.1.b to compare ISMS standards to answer the RQ2. Activity 2.2 illustrates the ISMS standards’ comparison (1.2.a) in the case process and results in 2.2.a.

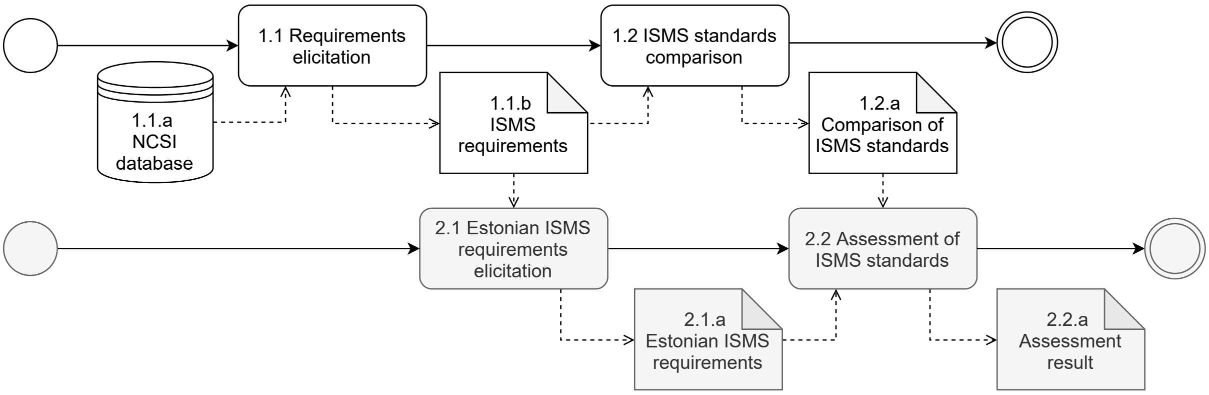
1.1 Requirements elicitation
1.2 ISMS standards comparison
1.1.a NCSI database
1.1.b ISMS requirements
1.2.a Comparison of ISMS standards
2.1 Estonian ISMS requirements elicitation
2.2 Assessment of ISMS standards
2.1.a Estonian ISMS requirements
2.2.a Assessment result

Figure 1. Study approach

3 Elaboration of ISMS Standards Requirements

3.1 Requirements Elicitation

NIS Directive [6] requires the EU member states to create and maintain national cybersecurity strategy and its implementation plan. National cybersecurity strategy is the fundamental source document for acceptable requirements of ISMS standards of the country among other strategic objectives.

For the security standard requirements elicitation we used the NCSI [14] database developed by the eGovernance Academy. eGovernance Academy collects links with publicly available evidence material of each country’s cybersecurity documents [14]. We wrote out the ISMS standard’s required properties of NCSI TOP 12 EU country’s cybersecurity strategy and implementation plan. Then we collected similar requirements under one requirement. We generalised the elicited requirements to cover different countries’ needs simultaneously. The requirements pass on the nature of the requirement, not the exact initial wording. Each requirement received the characteristic keywords. Finally, we got 15 requirements. We grouped the elicited requirements into three modules (see Table 1):

- **National security module** determines the national security aspects like compliance with jurisdiction regulations and the national authority right to make or influence to make changes into the content of the standard. This module allows assessing the possible future cost related to adoption and maintaining the ISMS standard. The target group of these requirements are the organisations responsible for ISMS standard development and maintenance on the national level.
- **Content module** helps to get to know the standard usability and adaptability issues related to implementation barriers and complexity. *Basic Controls* and *Levelled Controls* help to understand the implementation possibilities depending on the security needs. *Technology Dependence* and *Adaptability with National Needs* describe the flexibility of the standard controls. *Risk Management Approach* shows how risk management is included in the standard or requires separate management. The target group of these requirements are the organisations who have to implement the standard.
- **Assessment module** requires the monitoring and auditing capabilities to assess the organisation’s information security. The module characterises the needs and requirements outside the public sector. It is necessary to consider the availability and cost of resources like external certified auditors and audit bodies (target group of the module).

Each requirement received a unique ID (Nx, Cx or Ax) where x is a requirement sequence number and letter corresponds to the module the requirement belongs to. The county code in Table 1 shows the origin owners(s) of the requirement.

Table 1. National cybersecurity strategy requirements for ISMS standards

Req ID	Requirement	Requirement description	Country Code
National security module			
N1	**Developer and jurisdiction**	Standard should take into account EU and NATO regulations.	FI, GR, LT, HR
N2	**Development financing**	It should be possible to influence the development of the standard by national authority.	FI, GR, LT
N3	**Licence conditions**	Standard should be freely available to all national implementer.	FI, LT
N4	**Language**	Standard should be available in national language.	BE, GR, LT, LV
N5	**Update cycle**	Standards should be improved continuously/regularly.	BE, ES, GR, HR
Content module			
C1	**Scope**	Standard should be usable by public/private sector organisations information systems / processes / assets / critical infrastructure.	BE, CZ, ES, FI, GR, LT, LV, PL, SK, HR
C2	**ISMS compliance**	Standard should be compliant with internationally recognised standards / frameworks / best practices.	BE, CZ, ES, FI, FR, GR, LT, HR
C3	**Basic controls**	Standard should include basic/minimum security controls/measures.	BE, CZ, ES, FI, GR, LT, LV, PL, NL, HR
C4	**Leveled controls**	It should be possible to implement the standard controls/measures depending on the security level.	CZ, ES, FI, GR, LT, LV, PL, HR
C5	**Risk management approach**	Standard should include risk management.	BE, CZ, ES, GR, LT, LV, SK, HR
C6	**Technology dependence**	Standard should be technology-independent.	PL
C7	**Integrability of local needs**	It should be possible to adapt the standard with the national technological needs.	GR, PL
C8	**Controls approach**	It should be possible to change the content of the standard by national authority.	FI, GR, LT, PL
Assessment module			
A1	**Auditability**	Standard implementations should be auditable/assessable.	BE, CZ, ES, FI, GR, LV, PL, SK, HR, NL
A2	**Certification Schema**	Standard should be certifiable for being in compliance with recognized standards.	GR, PL, HR, NL

Estonian case ISMS requirements. We elicited Estonian requirements to ISMS standard from the Estonian Cybersecurity Strategy for 2019-2022 [17], the long-term Information Society Development Plan of Estonia (IÜAK) [18], and new ISMS standard procurement document [19]. These sources take into account the requirements of information security regulations.

Identified Estonian requirements are sorted according to Table 1. The result is given in the Table 3 columns *ReqID* and *Estonian Requirements*. Some of the identified Estonian requirements have been collected under same requirement ID, as their final objective is similar (e.g. N4, C1, C2). Also, some are mentioned more than once under several requirements, because they serve several goals (e.g., N2, C8 - one of them requires the possibility to make changes in the standard, the other requires controls approach and flexibility to add national aspects).

3.2 ISMS Standards Comparison Example

By following the requirements in Table 1, we compared the three following ISMS standards:

- **ISO27001** *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements* [20], developed by international level standardisation body and recognised globally.
- **CIS20** *CIS Controls v 7.1* [21], developed by industrial body, focuses only on information security. CIS20 provides TOP 20 security measures for organisations.
- **BSI ITG** *BSI IT-Grundschutz Kompendium* [22], differs from previous standards by its included threats, requirements and security controls catalogues. BSI ITG is known as a baseline security framework which is developed by an EU member state national standardisation body.

Standards content comparison CIS20 has published separate web articles of *CIS Mapping and compliance* to provide the control-by-control mappings to ISO27001, GDPR, and some industry specific frameworks [24]. BSI has published the analysis of BSI Standards and Kompendium compliance from the ISO27001 perspective [28]. These compliance confirmation publications assert that through ISO27001 perspective, three comparable standards contents cover the same security areas and are compliant to each other’s security objectives.

Standards comparison based on elicited requirements ISMS standards comparison results are presented in Table 2. The table gives a one-page overview of the similarities and differences of standards.

As the standard-setting similarities, we point out that the ISO27001 requirements and security objectives are reflected in other standards (C2). The standards are, thus, consistent with the security areas content. All three standards are intended to be used by a wide user community and do not impose restrictions to organisations by size, sectorality or industry field (C1). The introduction of risk management is required by all standards (C5). For all standards, there is one basic document supported by additional documents. It must be taken into account that the implementer must have all documents available (to take into account the cost to translation, maintenance, license fees) (C8, N4, N3, N5). None of the standard imposes restrictions on technologies directly (C6). An auditing and certification approach based on ISO27001 is suitable for all standards (A1, A2).

When deciding about standards, however, differences between standards become critical. For example, the chosen standards are part of different legal jurisdictions (N1) and there are also different funding schemes (at the moment: global, US, EU) (N2). Often, just through financing, it is possible to influence the content of the standards. This is important for national security considerations. The financing schemes of those three given standards differ by financier (national bodies, donations or state government) (N2). From the public sector’s perspective, it could be a problem if the standard has a license fee (ISO27001) and is not freely available (N3). To assess the standard dynamics or statics we can compare the update cycle

Table 2. ISMS Standards Comparison

Req ID	ISO27001	CIS20	BSI ITG
National security module			
N1	International Standardisation Organisation (Switzerland), globally recognised	Centre for Internet Security (US based non-profit organisation), US industrial, wide adoption	Federal Office for Information Security (BSI) (Germany), German national EU jurisdiction
N2	National bodies participate in development and finance ISO. Sale of standards. [25]	Contributors: US agencies, commercial partners. Financing: donations, grants, paid programs, product sales [26]	Publicly reviewed contributions. Financing: German Gov.
N3	User based fee (also to translated versions)	Free for registered users, Creative Commons	Free download
N4	20+ languages	English, Spanish, Italian, Japanese, Lithuanian, Estonian	German, English
N5	5 year cycle	No exact rule, expectation is yearly update	Every February 1st
Content module			
C1	No limitations	No limitations	No limitations
C2	Officially compliant with ISO/IEC Management system standards, Management system standards adopted from Annex SL of ISO/IEC Directives, Consolidated ISO Supplement.	ISO 27001, NIST Framework [23]	ISO 27001
C3	Requirements mandatory, objectives with justified exclusions	User profile Implementation Group (IG) based basic requirements	Basic protection
C4	No	Three IG based levels	Standard and High level
C5	Mandatory. Guidelines: ISO/IEC 27005, ISO 31000	Guidelines: CIS RAM, ISO 27005, NIST SP 800-39, RISK IT (ISACA)	Embedded. Extension: BSI Standard 200-3: Risk Management
C6	No	No	User profile based technology modules
C7	Through risk management, local implementation	Through risk management, local implementation	Through risk management, central new technical modules development. Process modules are compliant to German regulations
C8	Control objectives (14) and controls (114). Related: ISO27000 series (50+ standards). Important: ISO/IEC 27000, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005	Security mode: 3 Implementation Groups. Controls (20), subcontrols (171). Related: CIS Controls TM, CIS RAM	Security mode: Basic, Standard, Core. Security catalogue: process and technical modules(5+5), Submodules (94), 1680+ requirements and measures in modules. Related: IT-Grundschutz Compendium; standards BSI 200-1, 200-2,200-3; BSI 100-4
Assessment module			
A1	External audit based on ISO 27007	Self-assessment or auditing based on ISO27001 or other standards	External audit
A2	Based on ISO 27006, ISO 27007, ISO 27008	No	Based on ISO27001 requirements and BSI methodology

of standards (N5).

Organisations have different security needs and they are looking for matching security levels to optimise the security cost. So the organisations with lower security needs do not have to implement all the high-level measures. CIS20 and BSI ITG provide leveled approach (C3, C4). The volume of the guidance material can drive the usability of the standard (C8).

If ISO27001 and CIS20 are technology-free, then BSI ITG offers security measures suitable for the most common technologies (C6). Everyone can propose suitable profiles for the BSI, and if there exists a general approval, they will be integrated within a year into the composition of standard catalogues (C7, N5).

To summarize our comparison, the decision-maker should understand the differences and similarities of the standards, consider separately national security aspects (first module) and standards' content aspect (second module), and to weigh, how the auditing and certification schemes (third module) could work, and which resources are needed.

Estonian case standards assessment. From the perspective of the Estonian ISMS standard development it is important to compare the Estonian requirements with ISMS standards. In Table 3 we align the Estonian ISMS standard requirements with the compliance assessment to the three previously described ISMS standards (see Table 2). The qualitative sequence method has been used for the assessment: the most suitable standard in compliance with concrete Estonian requirement(s) is marked as “++”, suitable with some exclusions is marked as “v” and not suitable is marked as “0”, N/A is marked as “-”. We used the assessment mark “+” for interim cases of “++” and “v”. The result shows the differences between the standards in the National security module in Table 3. In the Content module the BSI ITG stands out with its positive results. In Estonian case the Assessment Module probably could not influence too much the decision making. The case shows that for Estonian public sector organisations, the most suitable standard to use is BSI ITG based standard.

4 Limitation and Conclusion

We investigated the national cybersecurity strategies and their implementation plans for requirements elicitation in their original languages using the Google Translate application (when needed). We avoided the progressing of the errors caused by machine translation by including the requirement in case ambiguity only if it appeared in both sources.

Second aspect to mention is that the national cybersecurity strategies are written in different detail and maturity levels. For example, the Greek documents covered 14 requirements out of 15, while we found only one requirement for the French public sector security. In order to bring the elicited requirements to the same maturity level, we ruled out very specific requirements for security measures and generalised them under Requirement ID C7. Also, the requirements are not with equal importance to national states. We suggest to assess them in the context of national objectives.

In the study, we elicited the ISMS requirements for public sector organisations in a form that supports reuse of the structured requirements. We used the structure of elicited requirements to compare three ISMS standards. In the example of the Estonian case, we showed how to compare requirements and standards. The result could be useful for small national states which wish to use the experiences and existing ISMS standards of other countries to develop their information security measures.

During the study, we perceived that all EU countries are simultaneously developing their standards or frameworks. Our working group came to the same conclusion with the ENISA report [13]. Hence the ENISA or other EU organisation could develop a central framework or baseline for public sector organisations security management, and each country could adapt

Table 3. ISO27001, CIS20 and BSI ITG standards assessment based on requirements to Estonian ISMS standard

(Notation: "++" - most suitable; "v" - suitable with some exclusions; "0" - not suitable; "-" - N/A; "+" - interim cases of "++" and "v")

Req ID	Estonian Requirements	ISO27001	CIS20	BSI ITG
National security module				
N1	Standard should enable the baseline security to fulfil requirements of national and international regulations like GDPR, NIS-directive, etc. [17].	v	0	+
N2	Standard should be flexible enough to add national content, measures or modules [19].	v	v	+
N3	Standard should be available free of charge [19].	0	+	++
N4	The standards must transfer Estonian language and culture, i.e. be in correct language, terminologically validated and compiled for Estonians [17]. Correct language and consistent terminology should be used and validated [19].	++	v	0
N5	Standard should be updated regularly/yearly [19, 17].	v	v	++
Content module				
C1	Information security should be integrated widely in all type of organisations and their processes [17]. Standard should be extendable for all public administration and industry organisations [17]. Standard should support public sector business processes [19].	++	++	++
C2	Standard should be based on an European or internationally recognised standards and practices [17, 6]. In case of a translation adoption, the standard should retain the connections with original document sets [19].	+	v	++
C3	Standard should help optimising risk management by providing predefined measures for typical solutions [19].	0	v	++
C4	Implementation process should enable levels of implementations - the base implementation and advanced levels based on security requirements [19].	0	+	++
C5	Standard should use and adopt risk based approach for information and network security management [17].	++	++	++
C6	All technologies should be given equal opportunities regardless of the platform [17].	++	++	+
C7	The obligation to use Estonian based technological solutions. Therefore, the standards must enable and propagate the use of X-tee and Estonian public key infrastructure (PKI) solutions. [19]	+	+	v
C8	Standard should be flexible enough to add national content, measures or modules [19].	0	0	+
Assessment module				
A1	Standard should allow audit-ability [19].	++	v	++
A2	-	-	-	-

them to their national regulations.

Acknowledgement. This paper is supported in part by EU Horizon 2020 research and innovation programme under grant agreement No 830892, project SPARTA.

References

[1] Purser, S., Standards for Cyber Security. In: Best Practices in Computer Network Defence: Incident Detection and Response, pp. 97–107. IOS Press, (2014), 10.3233/978-1-61499-372-8-97

[2] Oja, T., X-Road Trust Model and Technology Threat Analysis. (2020), Master Thesis, Tallinn University of Technology

[3] Mets, T., Parsovs, A., Time of Signing in the Estonian Digital Signature Scheme, In: Digital Evidence and Electronic Signature Law Review,16(2019), pp.40–50, https://doi.org/10.14296/deeslr.v16i0.5076

[4] Seeba, M., A Specification of Layer-Based Information Security Management System for the Issue Tracking System (2019), Master Thesis, Institute of Computer Science University of Tartu

[5] European Union, General Data Protection Regulation.(2018), http://eur-lex.europa.eu/. Last accessed 28 Jan 2021

[6] European Union, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, (2016), http://data.europa.eu/. Last accessed 22 Jan 2021

[7] Beckers, K., Côté, I., Fenz, S., Hatebur, D., Heisel, M., A Structured Comparison of Security Standards, (2014), 10.1007/978-3-319-07452-8_1

[8] Nabi, S., I., Al-Ghmlas, G., S., Alghathbar, K., Enterprise Information Security Policies, Standards, and Procedures: A Survey of Available Standards and Guidelines, In: Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions, pp.67–89, (2012), IGI Global, ISBN 978-1-4666-0197-0

[9] Tofan, D., Information Security Standards. In: Journal of Mobile, Embedded and Distributed Systems (3). (2011), ISSN 2067 – 4074

[10] Grandclaudon, J. (Ed.), D11.1 International and national cybersecurity certification initiatives. Report of SPARTA project. (2020), https://www.sparta.eu/. Last accessed 10 Jan 2021

[11] KPMG OY Ab, Digitaalisen turvallisuuden kansainvälinen vertailu Valtiovarainministeriö. (2020) https://vm.fi/documents/10623/307681/Digitaalisen+turvallisuuden+kansainv%C3%A4linen+vertailu/7aafe82e-86e7-7450-358c-f1adfeecb3e5/Digitaalisen+turvallisuuden+kansainv%C3%A4linen+vertailu.pdf. Last accessed 10 Jan 2021

[12] ENISA, Standardisation in support of the Cybersecurity Certification, (2020), 10.2824/481787

[13] ENISA, Good practices in innovation on cybersecurity under the NCSS, (2021), 10.2824/01007

[14] e-Governance Academy (eGA), NCSI National Cyber Security Index, (2021), https://ncsi.ega.ee. Last accessed 10 Jan 2021

[15] Ottis,R., Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective, Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf. Last accessed 10 Jan 2021

[16] Estonian Information Authority (RIA), X-tee factsheet, https://www.x-tee.ee/factsheets/EE/#eng. Last accessed 01 Nov 2020

[17] The Ministry of Economic Affairs and Communications of Estonian Republic, Cybersecurity Strategy Republic of Estonia 2019–2022, (2018). https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf. Last accessed 10 Jan 2021

[18] The Ministry of Economic Affairs and Communications of Estonian Republic, Infoühiskonna arengukava 2020, (2013) https://www.mkm.ee/sites/default/files/elfinder/article_files/eesti_infouhiskonna_arengukava.pdf. Last accessed 10 Jan 2021

[19] Estonian Information System Authority Public Procurement No. 203534. Development of the Estonian information security standard. Description of works. (2019) https://riigihanked.riik.ee/. Last accessed 1 Nov 2020

[20] International Standardisation Organisation (ISO), ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, (2013).https://www.iso.org/standard/54534.html. Last accessed 1 Nov 2020

[21] Center of Internet Security (CIS), CIS Controls, 2020 hhttps://www.cisecurity.org/controls/cis-controls-list/. Last accessed 20 Nov 2020

[22] German Federal Office for Information Security (BSI), BSI IT-Grundschutz Kompendium, 1-02-2020, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.html. Last accessed 10 Jan 2021

[23] German Federal Office for Information Security (BSI), BSI Standard 200-3: Risk Analysis based on IT-Grundschutz,(2017), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.html. Last accessed 10 Jan 2021

[24] Center of Internet Security (CIS), Mapping and Compliance. Collaboration Enhances Cybersecurity Compliance, https://www.cisecurity.org/cybersecurity-tools/mapping-compliance/. Last accessed 10 Jan 2021

[25] International Standardisation Organisation (ISO), Frequently Asked Questions (FAQS), https://www.iso.org/footer-links/frequently-asked-questions-faqs/general-faqs.html. Last accessed 20 Nov 2020

[26] Pro Publica Inc., Center for Internet Security Inc., Full text of ”Full Filing” for fiscal year ending Dec. 2019, https://projects.propublica.org/nonprofits/organizations/522278213/202041959349302934/full. Last accessed 10 Jan 2021

[27] Estonian Information System Authority (RIA), Three Level IT Baseline Security System ISKE, (2020), https://www.ria.ee/en/cyber-security/it-baseline-security-system-iske.html. Last accessed 10 Jan 2021

[28] German Federal Office for Information Security (BSI), Zuordnungstabelle. Zuordnung ISO/IEC 27001 sowie ISO/IEC 27002 zum modernisierten IT-Grundschutz, (2018) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Zuordnung_ISO_und_modernisierter_IT_Grundschutz.pdf?__blob=publicationFile&v=1. Last accessed 10 Jan 2021