

JYU DISSERTATIONS 826

Riku Nykänen

Supporting Control Selection in Information Security



UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION
TECHNOLOGY

JYU DISSERTATIONS 826

Riku Nykänen

Supporting Control Selection in Information Security

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi Agoran luentosalissa Alfa
lokakuun 3. päivänä 2024 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in building Agora, lecture hall Alfa, on October 3, 2024, at 12 o'clock.



JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2024

Editors

Marja-Leena Rantalainen

Faculty of Information Technology, University of Jyväskylä

Päivi Vuorio

Open Science Centre, University of Jyväskylä

Copyright © 2024, by the author and University of Jyväskylä

ISBN 978-952-86-0304-7 (PDF)

URN:ISBN:978-952-86-0304-7

ISSN 2489-9003

Permanent link to this publication: <http://urn.fi/URN:ISBN:978-952-86-0304-7>

ABSTRACT

Nykänen, Riku

Supporting control selection in information security

Jyväskylä: University of Jyväskylä, 2024, 80 p. (+included articles)

(JYU Dissertations

ISSN 2489-9003; 826)

ISBN 978-952-86-0304-7 (PDF)

Numerous organizations face challenges in determining the best way to ensure sufficient security measures to protect their operations and assets. Various standards and frameworks for information security management systems define sets of security controls to mitigate security risks. These security standards outline common security measures to be implemented, but only account for limited organizational variations. There exists a variety of different risk management methods to select optimal security controls; however, these methods usually require the use of resource-consuming assessments and expertise, which small and medium organizations often lack. Because information and cyber-security breaches are daily news, there is a need for practical approaches to risk management and security control selection.

This work uses design science research to develop a set of artifacts to pinpoint the most appropriate security controls based on the assets and security priorities of an organization. The included articles represent developed artifacts that support the selection of essential security controls, especially for SMEs. The results indicate that the use of preconditions for organizational aspects and priorities can support the selection of security controls to reduce the resource requirements for risk analysis and allow organizations to focus on the implementation of security controls. As part of this research, the design science research methodology is evaluated as a research method to develop information and cyber security assets. Overall, these results indicate that design science research provides efficient methods to develop practical artifacts for information and cyber security, but lack domain-specific validation criteria for developed artifacts.

Keywords: Information Security, Cyber Security, Risk Management, Risk Analysis, Security Control Selection, Design Science Research, Semantic Wiki, Knowledge Management

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Nykänen, Riku

Tietoturvallisuuden hallintakeinojen valinnan tukeminen

Jyväskylä: University of Jyväskylä, 2024, 80 s. (+artikkelit)

(JYU Dissertations

ISSN 2489-9003; 826)

ISBN 978-952-86-0304-7 (PDF)

Useat organisaatiot kohtaavat haasteita valitessaan riittäviä tietoturvallisuuden hallintakeinoja suojatakseen toimintaansa ja omaisuuttaan. Erilaiset standardit ja viitekehykset tietoturvallisuuden hallintajärjestelmille määrittelevät joukon tietoturvallisuuden hallintakeinoja riskien hallitsemiseksi. Nämä turvallisuusstandardit kuvaavat yleisiä turvatoimia, joita organisaatioiden oletetaan yleisesti toteuttavan, mutta ne ottavat huomioon organisaatioiden erilaiset ominaispiirteet vain rajallisesti. Hallintakeinojen valitsemiseksi on olemassa useita erilaisia riskienhallintamenetelmiä, mutta nämä menetelmät vaativat yleensä resursseja ja asiantuntemusta, joita pieniltä ja keskisuurilta organisaatioilla usein puuttuu. Koska tietomurroista on tullut arkipäivää kaikenlaisille organisaatioille, tarvitaan käytännönläheisiä menetelmiä riskienhallintaan ja tietoturvallisuuden hallintakeinojen valintaan.

Tutkimuksessa käytettiin suunnittelutiedettä menetelmänä kehittämään joukko artefakteja, joilla sopivimmat tietoturvallisuuden hallintakeinot voidaan valita organisaation suojattavien kohteiden ja turvallisuusprioriteettien perusteella. Sisällytetyt artikkelit esittelevät kehitettyjä artefakteja, jotka tukevat tietoturvallisuuden hallintakeinojen valintaa, erityisesti pk-yritysten näkökulmasta. Tulokset osoittavat, että huomioimalla organisaatioiden ominaispiirteet ja prioriteetit, voidaan tukea hallintakeinojen valintaa resurssivaatimusten vähentämiseksi riskianalyysissä ja mahdollistaa organisaatioiden kohdistaa resurssinsa varsinaisten hallintakeinojen toteuttamiseen. Tutkimuksessa myös arvioidaan suunnittelutiedettä tutkimusmenetelmänä tieto- ja kyberturvallisuuden kentässä. Tulokset osoittavat, että suunnittelutiede tarjoaa tehokkaita menetelmiä käytännönläheisten artefaktien kehittämiseen tieto- ja kyberturvallisuuden alalla, mutta toimialakohtaiset arviointikriteerit vaativat edelleen kehittämistä.

Avainsanat: Tietoturvallisuus, kyberturvallisuus, riskienhallinta, riskien arviointi, hallintakeinojen valinta, suunnittelutiede, Semantic Wiki, tiedonhallinta

Author	Riku Nykänen Faculty of Information Technology University of Jyväskylä Finland
Supervisors	Professor Tommi Kärkkäinen Faculty of Information Technology University of Jyväskylä Finland Docent Rauno Kuusisto Faculty of Information Technology University of Jyväskylä Finland
Reviewers	Professor Jukka Manner Department of Communications and Networking Aalto University Finland University Lecturer Ilona Ilvonen Faculty of Management and Business Tampere University Finland
Opponent	Professor Juha Röning Faculty of Information Technology and Electrical Engineering University of Oulu Finland

ACKNOWLEDGEMENTS

First, I would like to thank my supervisor Professor Tommi Kärkkäinen. Every time we discussed research, I felt very motivated to push research forward. This thesis would never be finished without his contribution, encouragement, and ideas.

I would like to thank my second supervisor, Dr. Rauno Kuusisto. His ideas gave new aspects to the research results. Also, his course on cyber security as a social system provided such points of view that no other course on cyber security can compete. I would like to thank coauthors of included articles, Mikko Hakuli and Tomi Kelo, for their insight and inspiring discussions.

As this thesis has been a long process, I would like to thank all my employers during these years, Relator Oy, Huld Oy, and TGR-WRT. Especially, I thank my former superiors and colleagues, Ph.D. Kimmo Kaario and Lassi Sutela, for support and flexibility during the lengthy process. I would like to show our gratitude to Olli Pitkänen for inspiring discussions during the Julkri development, which had a great impact on this dissertation. I also thank the University of Jyväskylä for allowing my doctoral studies.

I would like to thank my family and friends for their support and providing opportunities to clear my thoughts by doing something completely different. Thank you Jenni for your support that helped me complete this dissertation. Finally, I would like to thank my beloved children, Aino, Aura and Aaro, for support and infinite sarcastic comments. I truly hope this dissertation motivates you in your own studies in the future.

Thank you to everyone.

May 26th, 2024

Riku Nykänen

LIST OF ACRONYMS

AI	Artificial intelligence
C2M2	Cybersecurity Capability Maturity Model
CIA	Confidentiality, Integrity and Availability
CIS	Center for Internet Security
CSF	NIST Cybersecurity Framework
DK	Design Knowledge
DSR	Design Science Research
DSRM	Design Science Research Methodology
ENISA	European Union Agency for Cybersecurity
FEDS	Framework for Evaluation in Design Science
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
IMB	Information Management Board
IS	Information System
ISMS	Information Security Management System
ISO	International Organization for Standardization
KIBP	Knowledge-Intensive Business Process
KIBS	Knowledge-Intensive Business Services
MCDM	Multi-Criteria Decision-Making
NCSC-FI	National Cyber Security Centre Finland
NIST	National Institute of Standards and Technology
OSCAL	Open Security Controls Assessment Language
RMF	Risk Management Framework
ROI	Return of Investment
SCOR	Security and Privacy Control Overlay Repository
SME	Small and Medium-sized Enterprise
SMW	Semantic MediaWiki
UML	Unified Modeling Language
WSM	Weighted Sum Model

LIST OF FIGURES

FIGURE 1	Visualization of the main themes of the articles included	18
FIGURE 2	Security concepts and relations according to Common Criteria [48].....	20
FIGURE 3	The Julkri metamodel.....	30
FIGURE 4	The Julkri selection process of essential and optional criteria [6]	32
FIGURE 5	Design science research cycles by Hevner [39]	35
FIGURE 6	Components of design knowledge for a specific DSR project [9]	38
FIGURE 7	Knowledge utilization, production, and contribution to DSR [24]	39
FIGURE 8	DSR cycles with outcomes	49
FIGURE 9	Proposed process to utilize the knowledge base and the enhanced control catalogue	53
FIGURE 10	Core meta-model of the enhanced control catalogue.....	54
FIGURE 11	Control scoring classes	55

LIST OF TABLES

TABLE 1	Security risk management process phases [27].....	22
TABLE 2	New control attributes in ISO/IEC 27002:2022 [50].	27
TABLE 3	Julkri preconditions [6]	31
TABLE 4	Security control statistics	33
TABLE 5	Scoring class explanations	56
TABLE 6	Summary of the artifacts created in the research	59
TABLE 7	ChatGPT 3.5's responses to questions	78
TABLE 8	Copilot's responses to questions	79

CONTENTS

ABSTRACT

TIIVISTELMÄ (ABSTRACT IN FINNISH)

ACKNOWLEDGEMENTS

LIST OF ACRONYMS

LISTS OF FIGURES AND TABLES

CONTENTS

LIST OF INCLUDED ARTICLES

1	INTRODUCTION	15
1.1	Motivation for research	15
1.2	Research questions and main contributions.....	17
1.3	Structure of the thesis.....	18
2	BACKGROUND	19
2.1	Basic concepts in information security risk management	19
2.2	Information security risk management	21
2.3	Security control selection.....	23
2.4	Security control catalogs.....	25
2.5	Comparison of security control catalogs	32
2.6	SME challenges in information security	33
3	RESEARCH METHOD	35
3.1	Design science research.....	35
3.2	Knowledge in security risk management	37
3.3	DSR in information and cyber-security research	39
3.4	Knowledge-intensive business processes	40
4	SUPPORTING SECURITY CONTROL SELECTION	42
4.1	Security control semantics	42
4.1.1	Article I: Information security management system standards: A gap analysis of the risk management in ISO 27001 and KATAKRI	42
4.1.2	Article II: Comparison of Two Specifications to Fulfill Security Control Objectives	43
4.2	Enhanced control catalog	45
4.2.1	Article III: Tailorable Representation of Security Control Catalog on Semantic Wiki.....	45
4.2.2	Article IV: Supporting Cyber Resilience with Semantic Wiki	46
4.3	Evaluation of artifacts	48
4.3.1	Article V: Knowledge Interface System for Information and Cyber Security Using Semantic Wiki	48
4.3.2	Article VI: Analysis of the Next Evolution of Security Audit Criteria.....	50

5	DERIVED ARTIFACTS	52
5.1	Risk assessment process utilizing an enhanced control catalog	52
5.2	Control catalog object model	53
5.3	Control scoring model	55
5.4	Summary of artifacts.....	57
6	CONCLUSION	60
6.1	Results	60
6.2	Limitations	63
6.3	Future work.....	63
6.4	Epilogue.....	65
	YHTEENVETO (SUMMARY IN FINNISH)	66
	BIBLIOGRAPHY.....	68
	APPENDIX 1 CONTROL SELECTION USING AI.....	77
	INCLUDED ARTICLES	

LIST OF INCLUDED ARTICLES

- I Riku Nykänen & Mikko Hakuli. Information security management system standards: A gap analysis of the risk management in ISO 27001 and KATAKRI. *Proceedings of the 12th European Conference on Information Warfare and Security, ECIW 2013*, 344-350, 2013.
- II Riku Nykänen & Tommi Kärkkäinen. Comparison of two specifications to fulfill security control objectives. *Proceedings of the 13th European Conference on Cyber Warfare and Security, ECCWS-2014*, 150-159, 2014.
- III Riku Nykänen & Tommi Kärkkäinen. Tailorable representation of security control catalog on semantic wiki. *Cyber Security: Power and Technology*, 163-177, 2018.
- IV Riku Nykänen & Tommi Kärkkäinen. Supporting cyber resilience with semantic wiki. *OpenSym '16: Proceedings of the 12th International Symposium on Open Collaboration*, article 21, 2016.
- V Riku Nykänen & Tommi Kärkkäinen. A knowledge interface system for information and cyber security using semantic wiki. *Designing for a Digital and Globalized World, DESRIST 2018*, 316-330, 2018.
- VI Riku Nykänen, Tomi Kelo & Tommi Kärkkäinen. Analysis of the next evolution of security audit criteria. *Journal of Information Warfare*, 22(4), 25-39, 2023.

Riku Nykänen is the first author of all included articles and made the most significant contribution to each one. In addition to article writing, this included the analysis of data and the development of research artifacts. In developing Julkri, he helped develop the structure of the criteria and meta-model as part of the core team and supported the development of technical criteria. Other authors of the articles contributed to the writing and commentary, except for Article VI, in which Tomi Kelo contributed to the research and writing of the article. Additionally, other authors provided comprehensive guidance and information on the design and execution of each study with which they were affiliated.

1 INTRODUCTION

All organizations need to manage their information and cyber-security risks to ensure business continuity. For effective risk management, the essential question is which security controls an organization should implement to mitigate these security risks, as no organization has infinite resources to implement all the possible security controls. Small and medium enterprises (SMEs) even struggle with the implementation of fundamental information and cyber-security controls [18, 78] and therefore need practical support to achieve their objectives in information and cyber-security.

Design science research (DSR) has been used in information system research, but has rarely utilized information security artifact development, such as security control catalogs used to support information and cyber-security risk management. This thesis approaches the topic of the development of information and cyber security, especially in the SME context, using DSR methodology from a practical point of view. This chapter discusses the background and motivations, presents the research questions, and further explains the structure of this dissertation.

1.1 Motivation for research

Information security has been considered one of the most important issues on a company's agenda for more than a decade, because the increasing number of security breaches is a major threat to business operations and continuity [18, 28, 78]. The increase in security threats and vulnerabilities, combined with the lack of time and resources to effectively mitigate them in the business environment, highlights the importance of prioritizing risks and addressing the most critical ones [62]. In a survey by the European Union Cybersecurity Agency (ENISA), over 80% of SMEs stated that cyber-security issues would have a serious negative impact on their business within a week after the event, with 57% stating that they would most likely go bankrupt or out of business [78]. SMEs understand the need for information and cyber-security protection, but often lack the competence and

other resources to mitigate information and cyber-security threats [12]. The recent results of a survey by the Australian Cyber Security Centre indicate that almost half of SMEs spend less than 500 Australian dollars on cyber security per year [17]. In the same study, almost half of the SMEs rated their understanding of cyber security as "average" or "below average" and had poor cyber-security practices.

The efficiency of risk management and the security controls implemented are important not only to ensure an organization's own information and cyber security, but also to protect the privacy of personal data handled and to comply with privacy regulations, including the General Data Protection Regulation (GDPR) [69]. The GDPR requires organizations to implement appropriate technical and organizational measures to protect the personal data they process, necessitating a robust information security risk management process.

To protect their assets, such as information, information systems, or reputation, organizations implement security controls, also known as countermeasures. As early as 1970, the foundational Ware report [95] stated that comprehensive security requires a combination of hardware, software, communications, physical, personnel, and administrative procedural safeguards. Software itself cannot ensure the security of information if the operational environment is not otherwise secure; however, all mentioned aspects need to be taken into account. SMEs know they are struggling with security practices, but often do not know where to start [17]. Information security controls can be administrative, technical, or physical. Administrative controls include processes, policies, and, for example, security training. Technical controls include firewalls, endpoint protection software, and vulnerability management. Physical controls include, for example, physical access control and alarm systems. As no organization has infinite resources to implement all possible security controls, organizations need to select the security controls that suit their business needs and provide the best return on investment (ROI).

The number of security control catalogs, such as ISO/IEC 27002 [51] and NIST SP 800-53 [80], defines sets of security controls that organizations must evaluate and, if feasible, implement to ensure the protection of their assets. Although baselines exist, not only are SMEs struggling to implement important security controls, but also organizations in safety and cyber-security critical domains such as aviation [61] or public administration [89]. Although some investment in information security is good, more security is not always worth the cost [32]. It is not feasible for all organizations to have the resources to implement all the security controls defined in baseline standards but select only the controls providing a sufficient ROI. Especially for SMEs, it is not evident that they have the resources to implement a wide range of security controls, as even cyber-security-critical organizations struggle with implementation.

As SMEs struggle with resources, even low-cost controls can be an unattainable investment, especially if there is no executive management support for information and cyber-security protection [12]. However, information and cyber-security research rarely focuses on SMEs, despite the fact that they represent a large proportion of businesses [13]. SMEs represent 99% of EU companies and occupy two-thirds of private sector employees, and the sector generates 58,4% of

the gross value added [60]. However, in SME organizations, there is rarely a dedicated staff to continuously maintain and monitor information and cyber-security, leading to personnel multitasking and a lack of time to focus on security activities, contributing to security weaknesses [78]. The importance of SMEs to society has also been noted in the recent EU Cyber Security Directive NIS2 [23], where one of the requirements for national cyber-security strategies is to strengthen the cyber resilience and cyber hygiene baseline of SMEs. In response to increasing cyber-security regulations, SMEs expect the public sector to provide funding and resources to implement cyber-security measures [75].

Because no two organizations are the same, modern approaches to information and cyber-security risk management require organizations to utilize risk management methodology to analyze assets, threats, and risks. Based on the results of the assessment, organizations select the security controls they need to implement to mitigate risks to an acceptable level. There exist a variety of quantitative security risk management methods that support organizations in their selection of security controls. However, these require the existence of numeric input data, such as risk realization statistics, life-cycle costs of controls, and proper asset valuation, to provide accurate results [81]. SMEs often lack the competence and input data required to select optimal security controls based on risk assessment without external assistance and expertise [13]. It is not merely a question of resources, because even security professionals can realize different results in risk assessment due to human factors [79]. In addition, cyber-security analytics solutions cannot take into account the specific needs of SMEs such as the limited ability to invest in security solutions [83]. SMEs also have problems correctly implementing the selected security controls [2].

1.2 Research questions and main contributions

This dissertation approaches information security risk management from a practical point of view to develop a demonstrator to support organizations in their information security risk management. The research questions combine the evaluation of the artifact and the DSR methodology used.

RQ1 How can security control catalogs be enhanced to support SME organizations' information and cyber security, especially in security control selection, without a complex risk assessment process?

RQ2 Under what conditions can the DSR methodology be utilized in the development of information security artifacts?

Instead of finding complex metrics, it is more critical to focus on security risk management and identify assets that have an impact on an organization's business continuity. This research represents a practical demonstrator for an enhanced security control catalog, which especially supports SMEs in identifying relevant

security controls based on a simple analysis of their assets and related risks. Compared to the traditional control catalog approach with no or limited prioritization between controls, the demonstrator supports organizations to identify potential controls from a more limited set of controls and focus their security risk management work more efficiently.

The results of the demonstrator were used in the development of the Julkri criteria [6]. Julkri was developed in coordination with the Finnish National Information Management Board (IMB) to assess compliance with the Act on Information Management in Public Administration [1]. Compared to its predecessors, Julkri contains a new type of selection logic of essential and optional security controls for assessment. This is required because Julkri needs to scale from the smallest Finnish municipalities and their service providers to ministries and large cities, which have varying needs and resources for information security.

As the focus of the research was the development of new demonstrative artifacts, the design science research methodology (DSRM) was found to be suitable for the evaluation of the artifacts, although it has been used only concisely in information security research. As part of the research, the suitability of DSRM for information security research was evaluated.

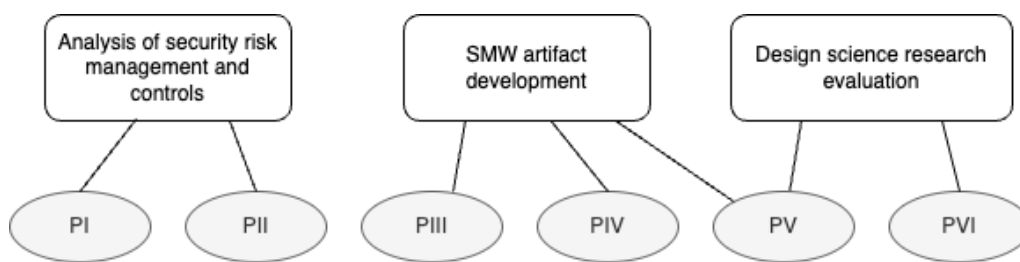


FIGURE 1 Visualization of the main themes of the articles included

The included articles compose three pairs, each pair having a specific theme. Articles I and II cover the background analysis of the risk management requirements and security controls required to support the further research and development of the artifacts. Articles III and IV cover the development of the wiki-based information security knowledge base and the risk management tool. The last two articles, Articles V and VI, focus on the evaluation of artifacts and the evaluation of the DSR methodology in information and cyber-security research. Figure 1 presents the main themes of the articles included.

1.3 Structure of the thesis

This dissertation is structured as follows. Chapter 2 provides an introduction to information and cyber-security risk management and security controls. Chapter 3 represents the used research method, and Chapter 4 contains a summary of the included articles. Chapter 5 presents additional results not included in the articles. Finally, Chapter 6 concludes the dissertation.

2 BACKGROUND

Information security risk management is a systematic approach to identifying, assessing, prioritizing, and mitigating risks that could compromise the confidentiality, integrity, and availability of an organization's information assets.

2.1 Basic concepts in information security risk management

It is essential to understand the terms of information security risk management and their relationships. There exist several different information security ontologies, however, Common Criteria (CC), also known as ISO/IEC 15408 [48], concepts have been widely adopted for use in ISO/IEC and other standards. Key concepts are as follows:

Definition 1. *An **asset** is an item, thing, or entity that has potential or actual value to an owner [46].*

Definition 2. *A **risk** is the effect of uncertainty on objectives [46].*

Definition 3. *A **control** (countermeasure) is a measure that modifies risk [49].*

Definition 4. *A **threat** is a potential cause of an unwanted incident, which may cause harm to a system or organization [49].*

The relationships of the most important concepts are presented in Figure 2. Typically, the organization is the owner of the assets, where the assets range from intangible entities such as competence or software to tangible assets such as physical devices. As in information and cyber security, the concept of an asset includes everything that has value for its owner, which is a more generic definition than in risk management, where some taxonomies use a three-level definition of a business, service, and asset [81, 76]. In information and cyber-security risk management, business and service entities are also assets if they provide value to the owner.

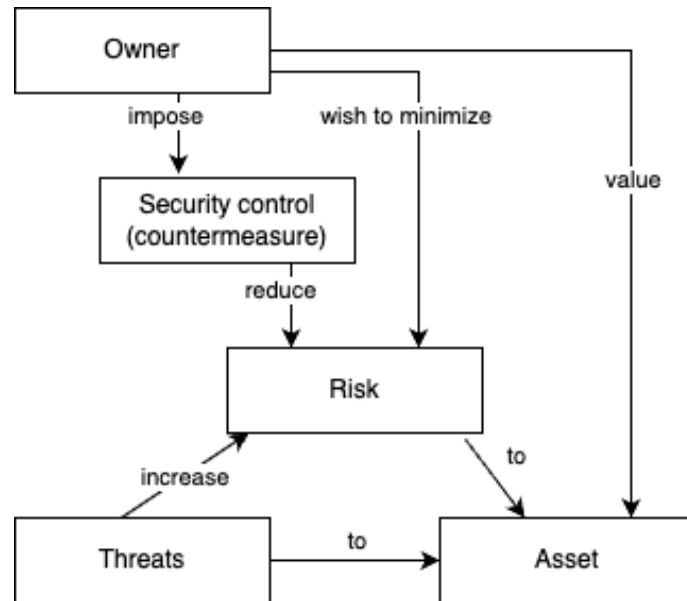


FIGURE 2 Security concepts and relations according to Common Criteria [48]

There exist several generic and domain-specific threat taxonomies, which categorize information and cyber-security threats [54, 76]. The German information security specification IT-Grundschutz includes the Compendium [52], which is a unique information and cyber-security specification as it contains, in addition to security controls, lists of typical threats and assets. It also includes a cross-reference to map elementary threats to the security controls that mitigate the threats. Threat taxonomies can be used in risk assessment to verify that specific threats are not ignored. In general, threat catalogs can be organized as a hierarchy of threats where threats are also associated with one or more information security attributes: confidentiality, integrity, or availability [29].

The risk is an entity between an asset and a threat. The common understanding of risk in the security community is captured by the so-called three-factor perspective, which aggregates the value, threats, and vulnerabilities of the asset [5]. This does not include the element of uncertainty as in the definitions of ISO standards [49, 46], which is usually taken into account as the probability of the realization of the risk. In ISO/IEC 27005, a security risk is measured as a tuple of impact of the realized risk and the probability of risk realization.

Security control is a countermeasure to mitigate security risks. Security controls can be divided into three groups and general levels [53]:

- *Management*: actions taken to manage the development, maintenance, and use of information systems, including policies and procedures.
- *Operational*: everyday mechanisms to protect operational systems and the environment, including awareness training, configuration management, and incident response.
- *Technical*: hardware and software controls used to protect systems and information.

From the point of view of impact and likelihood, security controls can be classified as preventive, detective, and corrective [51]. Preventive controls reduce the probability, and detective and corrective controls reduce the impact of the realization of the risk.

Security control catalogs are collections of security controls. In information security management, security control catalogs are often used to demonstrate compliance. Compliance can be described as the act of fulfilling expectations and, more precisely, compliance is verifiable consistency with clearly defined rules [21]. Information security assessment is the evaluation process to verify compliance with the set of rules. The evaluation criteria used in the assessment to establish the set of rules. Information security audits can have multiple types or targets, from organizations to specific products. Where the widely used ISO/IEC 27001 Standard is the audit requirement specification for an information security management system (ISMS), other specifications originate from different backgrounds like, for example, from regulation or technology. Hence, it is important to select a control catalog that is appropriate for the goals of the organization.

2.2 Information security risk management

Modern ISMS standards and specifications, such as ISO/IEC 27001 [50] and NIST SP 800-53 [80], are risk based, meaning that there is no specific information security control set to implement, but organizations select the security controls that are optimal for their risk landscape. The optimal selection of security controls is also the main goal of most risk management methods [25]. Optimal security control selection requires organizations to identify their security risks and threats and, based on the results, select the security controls to be implemented.

To support the implementation of the security risk management process, there are multiple widely adopted security risk management methodologies, such as ISO/IEC 27005 [47], which is related to the ISO/IEC 27001 Standard. Fenz and Ekelhart [27] have identified the common phases and outcomes of five different security risk management methods: CRAMM, NIST SP 800-30, OCTAVE, EBIOS, and ISO 27005. The generic phases and outcomes are presented in Table 1.

As the generic phases show, organizations need to identify the assets they wish to protect, identify the threats (risks) related to the assets, and select security controls to protect the assets. Sufficient asset identification and valuation in the first phase can be seen as a prerequisite for the successful completion of the following phases [29]. If the organization does not identify the assets, it cannot reliably identify the risks facing the assets and can fail to select the mitigating controls effectively. In addition, if the organization fails to value the asset incorrectly for its operation, effective control selection can fail or lead to infeasible investments. The security risk management process is usually not linear but iterative, as reviewing threats and potential controls may help identify new assets to be protected and can result in the assessment of new risks.

TABLE 1 Security risk management process phases [27]

Phase	Output
System characterization	List of assets that need to be protected and their acceptable risk level.
Threat and vulnerability assessment	Inventory of threats and associated vulnerabilities that endanger identified assets.
Risk determination	Quantitative or qualitative risk metrics and levels of identified threats.
Control identification	A list of possible controls that can reduce risks to an acceptable level.
Control evaluation and implementation	A list of cost-effective security controls that must be implemented to mitigate risk to an acceptable level.

A risk analysis is performed to assess risk characteristics, such as probability and impact, and to assess potential security controls. Risk analysis methods are quantitative, semiquantitative, or qualitative techniques to determine the level of risk. The common way to perform a risk assessment is to use a qualitative risk matrix approach. In traditional qualitative analysis, the risk score is the result of the evaluation of the probability and impact tuple. Although the goal is to identify risks with a risk score that exceeds the acceptable risk appetite, risk matrices also have potential problems, as they have limited ability to correctly reproduce the risk ratings implied by quantitative models [16]. For example, failed estimates of the occurrence or impact of the risk will cause organizations to ignore critical risks and focus on irrelevant risks. In addition, qualitative risk analysis is always the result of human opinions, which tend to lean toward overoptimism and an unbalanced focus between probability and impact [71]. There are multiple studies on optimism bias in risk assessment in which people discount the likelihood of negative security events [63]. Common challenges also include risk prediction, a lack of understanding and the overconfidence effect, knowledge sharing, and risk versus cost trade-offs [29].

Various quantitative or semi-quantitative risk assessment methods also exist. In quantitative risk assessment, the risk of each scenario is estimated numerically using a quantitative model and measures. The use of quantitative methods usually requires complex metrics, and therefore, simple qualitative methods are often preferred. Moreover, many of the self-described quantitative methods are semi-quantitative methods that use numerical values based on the expert's opinion, which can be subjective and unrepeatably [25]. For example, a reliable analysis of the impact of a realized risk in a supply chain would require a complex model that takes into account multiple characteristics of modern supply chains. In addition, such an analysis would need to have clear and adequate quantitative measures to provide reliable results [7]. Due to limited data and challenges with modeling the dynamic aspects of threats and vulnerabilities, many quantitative methods to determine security risks are also inherently flawed [25]. Quantitative methods must balance efficiency and accuracy, which favors either of them [94]. When

preliminary and high-level risk assessment is required, efficient quantitative methods are more suitable, and more complicated methods need to be used when the priority is the accuracy of results.

In addition to qualitative and quantitative risk management methods, there are also maturity model-based approaches to security control selection [79]. For example, the COBIT framework enables us to assess the prevailing security situation in an organization. The Finnish national Cybermeter [59] developed by the National Cyber Security Centre (NCSC-FI), the NIST Cybersecurity Framework, and the Cybersecurity Capability Maturity Model (C2M2) [19] are also maturity model based. In maturity model-based assessments, organizations assess the maturity level of important operational security capabilities, usually per domain and objective. A maturity model provides a reference point for the current level of organizational practices, processes, and methods and sets goals and improvement priorities. Many of the capabilities evaluated are the existence of common security processes such as the risk management or implementation status of common security controls, for example, vulnerability management. Hence, maturity models do not reinvent the wheel, but provide another approach to assess and develop information and cyber security. From an SME point of view, the maturity model requires similar resources, especially information security knowledge, to provide meaningful assessment results.

Security controls may be administrative, such as policies and training, or technical, such as endpoint protection software and backup. In their conclusion of the systematic review of the literature, Bekkevil et al. [8] noted that effective information security requires not only appropriate technical solutions, but also sound information security practices. Training and organizational collaboration at different organizational levels are the two most discussed types of security initiative. Although many organizations have administrative and technical controls in place, these organizations must also consider employee attitudes, knowledge, and behavior when selecting appropriate security controls [8]. Furthermore, technological developments have an impact on the security controls that organizations need to implement, and evolving technologies can cause problems, especially for SMEs [2]. Cloud services have become more popular during the last decade and possess different types of threat than the on-premise services they are replacing [90]. From a security risk management perspective, organizations must adapt their security controls to changing asset outlooks.

2.3 Security control selection

The goal of selecting security controls is to identify the controls that will provide the best expected ROI for the organization to mitigate the identified risks. There exist different methods to select security controls, where simple methods include ordering the security controls from the best to the worst using pairwise comparison [64]. For optimal security control selection, a predictive model is needed to identify

how a control modifies all risks and threats [71]. As risks and controls have complex dependencies and difficult-to-observe effects, it is not realistic to expect that control selection would be optimal even if an organization has the necessary resources, since control efficiency is expected to change over time [71]. As all organizations are different, risk-based methods aim to find the optimal security controls for the current organization, for current protectable assets, and/or for a more strictly specified use case. For large organizations, it might not be feasible to implement an organization-wide security control, but only for selected valuable assets.

In compliance requirements, the common approach is to review the reference control set. ISO/IEC 27001 requires organizations to *“determine all controls that are necessary to implement the information security risk treatment option(s) chosen”* and compare those controls with Annex A that so no necessary controls have been omitted [50]. Annex A refers to the annex of the standard that contains security control objectives and controls presented in detail in the ISO/IEC 27002 Standard. Furthermore, it is noted that *“control objectives and controls listed in Annex A are not exhaustive, and additional control objectives and controls may be needed.”* Such a situation could be the usage of recently emerged technologies such as, for example, artificial intelligence (AI), which is not covered by the controls of the latest version of ISO/IEC 27002. The risk-based approach of ISO/IEC 27001 can be characterized as a risk assessment based substantially on a review of the control catalog. In addition, measuring the efficiency of a security control can be difficult and require overly simplified numeric estimations [71]. For technical security controls, it is often easy to detect that the control is working and protecting assets. However, the evaluation of organizational controls, such as security training, is harder, especially before training implementation, as it will depend on multiple factors such as personnel motivation, training quality, and coverage [12].

It has been identified that large amounts of control options and the amount of information become counterproductive, basically making things worse that is, less secure [36]. The term Fog of More is used to describe the state in which organizations have so many options, policies, and services that it is easy to become paralyzed. Many organizations have too many security solutions to effectively manage them all, leading security professionals to have too much noise to distinguish critical security alerts from systems [77].

The available resources of the organization also have an impact on the selection of security control. Where organizations with better resources are able to implement partially overlapping controls to ensure the principle of defense in depth to prevent security breaches, even single security controls would fail, or there would be cases of human errors [15]. Conversely, organizations with limited resources struggle to implement even the most critical controls due to a lack of resources and management commitment [12]. The more limited resources an organization has, the more important it is to select the security controls that mitigate the overall risks to the greatest extent. To identify these controls, organizations can review different options in different security control catalogs.

2.4 Security control catalogs

There exist a number of different information and cyber-security management frameworks and control catalogs. Selecting the relevant applied framework, including the security control catalog, is primarily a business decision based on the organizational context and risk profile, which needs to consider the applicable laws and regulations [58]. Next, five security control catalogs used in the included articles are presented, after which catalogs are compared from a statistical perspective.

NIST SP 800-53

The Special Publication (SP) 800-53 "Security and Privacy Controls for Information Systems and Organizations" from the National Institute of Standards and Technology (NIST) has been primarily created to help US federal agencies, but is also applied by the private sector [80]. It is currently in its fifth revision (rev5) published in September 2020.

From a structural point of view, NIST SP 800-53 consists of 20 control families. SP 800-53 has a two-level control structure, where controls can have control enhancements as subelements defining additional details. NIST SP 800-53 contains four security baselines: low, moderate, high, and privacy. The security baselines are used to classify systems and organizations based on their criticality and to filter the control set to the appropriate level to meet the required security level. The definitions of low, moderate, and high baselines are based on the security impact levels defined in the federal standard FIPS PUB 199 [87]:

Definition 5. *The potential impact is **low** if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.*

Definition 6. *The potential impact is **moderate** if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.*

Definition 7. *The potential impact is **high** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.*

The privacy baseline defines the security controls to be applied when personal data is processed. In such a case, the relevant set of controls is the union of the appropriate impact level controls and privacy baseline controls.

The NIST Risk Management Framework (RMF) includes the Security and Privacy Control Overlay Repository (SCOR) [66], which provides stakeholders a platform for sharing control overlays. An overlay is a set of controls that are applicable to a specific system or situation. The overlays are created by subject matter experts to help reduce the duplication of effort and share best practices for

specific use cases. An overlay may include controls from more than one catalog, and therefore, overlays are not limited to utilize controls only in NIST SP 800-53. SCOR contains overlays, for example, for physical access control systems, federal PKI Systems, and ICT supply chain risk management.

The NIST SP 800-53 release 5 security controls catalog is available in XML format, which follows the Open Security Controls Assessment Language (OSCAL) schema. OSCAL defines machine-readable representations of control catalogs, control baselines, system security plans, and assessment plans and results. OSCAL is a set of formats expressed in XML, JSON, and YAML [68]. These representations can be used to efficiently transform specifications to other data formats compared to specifications that are released only in document format, such as ISO/IEC 27002.

ISO/IEC 27002

ISO/IEC 27002, titled "Information Security, Cybersecurity and Privacy Protection – Information Security Controls", is an international standard that provides guidance on the normative security controls defined in Annex A of ISO/IEC 27001 [50]. ISO/IEC 27001 defines requirements for the Information Security Management System (ISMS), and the organization can obtain certification against the requirements. As a part of the information security risk treatment requirements, ISO/IEC 27001:2022 states that an organization shall compare the controls it has determined to implement to the control in Annex A and verify that no necessary controls have been omitted.

In ISO/IEC 27001 Annex A, the control listing contains only the control identifier, a title, and a short description. ISO/IEC 27002 provides more detailed guidelines and other relevant information to support the control implementation. The security controls are grouped in to four clauses:

- Organizational controls
- People controls
- Physical controls
- Technological controls

In the latest version, ISO/IEC 27002:2022 has added five new attributes to the controls compared to the previous version: control type, information security properties, cybersecurity concept, operational capabilities, and security domains. The attributes are designed to enable the creation of customized perspectives of a control catalog to support the selection of suitable subsets of controls. The new attributes are represented in Table 2.

Each of the controls has one or more values for each attribute. New attributes are especially encouraged to be implemented to speed up the risk treatment process [51]. ISO/IEC 27002:2022 states that organizations can not only omit the attributes but also introduce their own attributes and assign controls with the relevant values.

TABLE 2 New control attributes in ISO/IEC 27002:2022 [50].

Attribute	View point	Possible values
Control type	Attribute provides the perspective of when and how the control modifies the risk.	Preventive, Detective, and Corrective.
Information security properties	Characteristic of information the control will contribute to preserving.	Confidentiality, Integrity, and Availability
Cybersecurity concept	Cybersecurity concepts defined in the cybersecurity framework described in ISO/IEC TS 27110.	Identify, Protect, Detect, Respond, and Recover.
Operational capabilities	Practitioner's perspective of information security capabilities.	*
Security domains	Information security domains.	Governance and Ecosystem, Protection, Defense, and Resilience.

* Possible operational capability values are Governance, Asset_management, Information_protection, Human_resource_security, Physical_security, System_and_network_and_vulnerability_management, Continuity, Supplier_relationships_security, Legal_and_compliance, Information_security_event_management, and Information_security_assurance.

Annex A also provides a list of possible organizational attributes:

- a) maturity (values from the ISO/IEC 33000 series or other maturity models);
- b) implementation state (to do, in progress, partially implemented, fully implemented);
- c) priority (1, 2, 3, etc.);
- d) organizational areas involved (security, ICT, human resources, top management, etc.);
- e) events;
- f) assets involved;
- g) build and run, to differentiate controls used in the different steps of the service life cycle; and
- h) other frameworks the organization works with or can be transitioning from.

Compared to previous versions of ISO/IEC 27002:2022, the new attributes and related guidance improve the support of the control selection. However, the prioritization of controls still remains the responsibility of the user as new attributes support the filtering of the controls.

The widely used international standards ISO/IEC 27001 and 27002 have also been a basis for different specific guidelines. In the SME context, an interesting application is the SME Guide on Information Security Controls [86] by Small Business Standards (SBS). SBS is the association representing European SMEs' interests

in standardization. Although the guideline was published in 2022, it refers to the ISO/IEC 27002:2013 version, from which it recommends the implementation of 16 controls to ensure minimum effective protection of enterprise's data. Controls and other recommendations aim to reduce the risks assessed and therefore provide guidelines for applying the ISO/IEC 27001 risk management process [85]. Although the guidelines provide a starting point to implement security controls, they only provide a limited roadmap to develop information security, since the only prioritization aspect is the type of organization as an SME and therefore does not solve the scalability problem of ISO/IEC 27002.

CIS Controls

The author of CIS Controls [14] is the community-driven nonprofit organization Center for Internet Security (CIS). CIS Controls does not have the status of a national or international standard, but is widely adopted as a reference control set. The origin of CIS Controls is in expert community work in mapping summaries of attacks into the required defensive controls. CIS Controls is available as a PDF document and in Excel format.

From a semantic point of view, CIS Controls' current Version 8 has 18 controls. All of the controls contain more detailed safeguards. Therefore, a control is similar to a control family in NIST SP 800-53, a concept to group safeguards, although it contains an explanatory section. Each control has a short overview and two sections with a description: "Why is this control critical?" and "Procedures and tools." CIS also provides a mapping of CIS Controls to other numerous specifications, including ISO/IEC 27001, ISO/IEC 27002, NIST SP 800-53, and the NIST Cybersecurity Framework (CSF) [30].

To prioritize the implementation of the safeguards, the safeguards are divided into three implementation groups. Implementation groups have been introduced to fight against the fog of war, that is, having too many controls to implement that lead to overlapping and infeasible investments instead of building security based on the maturity of the organization [77]. Although prioritization is simple, it is complemented by two safeguard attributes. The asset type describes the kind of asset that the safeguard primarily protects. It contains only a single value for each safeguard, where possible values include users, data, applications, devices, and networks. In addition, some safeguards do not have a specific primary protected asset type, for example, security awareness-related safeguards. The second attribute is the security function, which also has one value per safeguard. The security function values are derived from the NIST CSF and include identify, detect, protect, respond, and recover.

Unlike other specifications presented, CIS has published a separate implementation guide for SMEs [31], which includes guidance on implementation group 1 (IG1) safeguards. By definition, IG1 contains the essential safeguards and represents a minimum standard of information security for all enterprises. The guide is divided into six phases, each of which contains a set of instructions, lists of actions to take, and references to supporting material and additional guidance. However,

the phases or guidance is not directly mapped to the CIS Controls safeguards, but following all phases will eventually lead to the implementation of the majority of the IG1 safeguards.

Katakri

The Information Security Audit Tool for Authorities (Katakri) is aimed to assess the protection of national and EU classified information [55]. It has been created in close cooperation between Finnish governmental security authorities and the private sector. Katakri is used mainly for three purposes: to meet the requirements of international treaties, to improve the procurement and operation of critical government systems, and to assess the reliability of the government supply chain [55, 72]. It covers the national and corresponding EU security classification levels Restricted, Confidential, and Secret. Requirements to process the information classified with the highest Finnish national security classification, Top Secret, are excluded from Katakri.

As Katakri defines requirements to process security classified information, it uses the term requirement instead of security control. However, requirements often relate to the security control definition in ISO/IEC 27002 and NISP SP 800-53. The requirements are prioritized according to the security classification of protected information. The latest version, Katakri 2020 [55], categorizes requirements into three subdivisions: security management, physical security, and information assurance. Structurally, Katakri contains long description text for each control, which may include multiple requirements for different security levels. As Katakri's background is in national regulation, each requirement also contains a reference to the corresponding legislation.

Katakri is available in document and Excel formats, which is more structured than document specifications. In the Excel version, it is possible to filter requirements based on the security classification level. For control selection, Katakri is the most limited as the security classification is basically only the attribute use in addition to three sections of the specification. However, requirements have been established to allow different implementation options and to facilitate interpretation. Examples of implementation have been compiled in the Additional Information field of each criterion. The field contains examples of procedures to meet the minimum protection requirements in most cases [55].

Julkri

Julkri criteria were initially published in 2022 to support compliance assessments of the Act on Information Management in Public Administration [1]. The Act defines obligations relating to information security measures that apply to information management units and authorities as well as their service providers also in the private sector. Julkri describes the assessment criteria for information security in public administration (Julkri) and provides instructions for using them. It also supports compliance assessments of the Government Decree on Security

Classification of Documents in the Central Government [34].

The initial content of Julkri is based on Katakri. However, compared to it, Julkri introduced a new approach to security control selection using preconditions. Where control selection in the predecessors of Julkri has been based only on the security classification of the information, Julkri contains more preconditions to select effective audit criteria and an applied set of controls. As Julkri users include the smallest municipalities and their service providers in Finland, the control selection logic needed to scale from all differently sized public and private sector entities. Therefore, it was expected that all Julkri users would not be information security experts but have limited information and cyber-security competence. In Julkri's development, considerable effort was invested into developing a new kind of selection logic that would also suit organizations with limited security expertise. Figure 3 represents the Julkri metamodel as a UML model, where the class "Assessment criteria" comprise the preconditions.

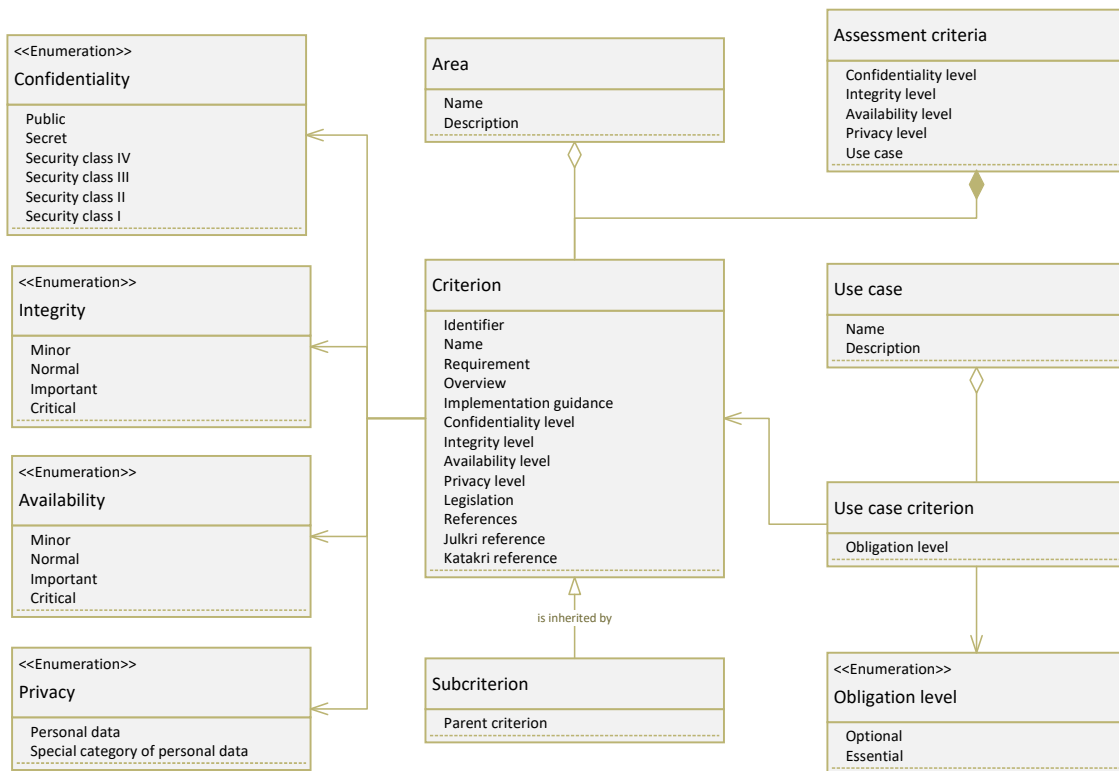


FIGURE 3 The Julkri metamodel

The Julkri user defines preconditions to select essential and optional criteria. The preconditions include an information security classification following Finnish national security confidentiality levels as well as information integrity and availability requirements. The preconditions also include the privacy aspect if the assessment target processes personal data. There is also an optional precondition that defines the use case, which is a similar concept to OSCAL overlays. In addition to four predefined use cases, user organizations can define their own use cases, for example, to assess service providers. Table 3 presents the preconditions and their possible values.

TABLE 3 Julkri preconditions [6]

Property	Description	Possible values
Confidentiality	Confidentiality levels are Finnish national security confidentiality levels.	<ul style="list-style-type: none"> • Public • Secret • TL IV • TL III • TL II • TL I
Availability	Availability level refers to how information, an information system, or a service can be used at the desired time and in the required manner.	<ul style="list-style-type: none"> • Minor • Normal • Important • Critical
Integrity	Integrity is a characteristic of information that means that the information has not been altered without authorization or that it has not been altered accidentally and that any changes can be verified.	<ul style="list-style-type: none"> • Minor • Normal • Important • Critical
Personal data	Personal data level contained by the system or service.	<ul style="list-style-type: none"> • None • Personal data • Special categories of personal data
Use case	Predefined set of criteria suitable for a specific situation.	<ul style="list-style-type: none"> • Administrative security assessment of the information management unit • Assessment of an SaaS cloud service • Procurement of expert work • Assessment of the production of information system services

The Julkri tool uses preconditions to select effective criteria for specific security assessments. Initially, the Julkri tool was released as an Excel worksheet, but later was released also as an SaaS service to Finnish national public sector organizations required to comply with the Julkri requirements. Figure 4 represents the selection logic of essential and optional criteria.

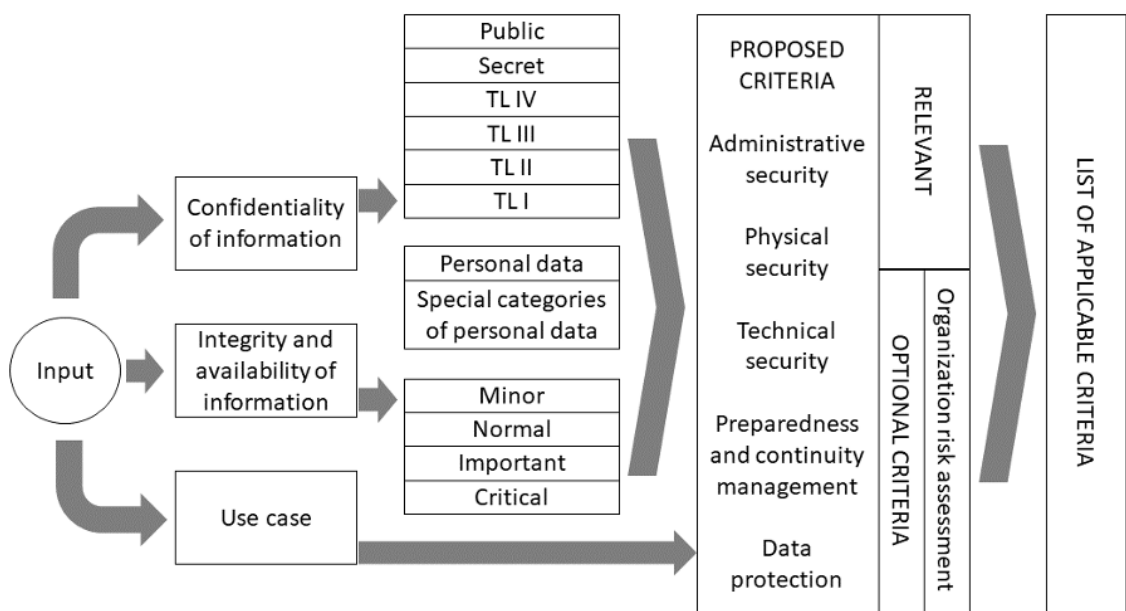


FIGURE 4 The Julkri selection process of essential and optional criteria [6]

Julkri contains a similar two-level structure in which criteria can have sub-criteria for NISP SP 800-53 control and control enhancement. The criteria are divided into five sections: (1) administrative security, (2) physical security, (3) technical security, (4) preparedness and continuity management, and (5) data protection. If the preconditions state that the assessment target does not process personal data, then no criteria from the data protection section are selected. The effective criteria contain relevant and optional criteria. The relevant criteria are expected to be met, or compensatory controls must be presented to comply with the criteria. The optional criteria leave room for organizations' own risk assessment whether to implement them or not.

2.5 Comparison of security control catalogs

The security control catalogs presented originate from different backgrounds and, as shown, have structural differences. Moreover, the number of controls is different. Table 4 represents statistics on controls in the four presented control catalogs, also showing the number of controls at different priority levels.

Julkri contains 768 different alternatives to define preconditions with four predefined use cases. Therefore, Table 4 contains only the minimum and maximum subset values. NISP SP 800-53 is the most extensive control catalog with a total

TABLE 4 Security control statistics

Specification	Statistics
NIST SP 800-53	20 control families containing 298 controls and 709 control enhancements Low Profile: 131 controls, 18 control enhancements Moderate Profile: 177 controls, 110 control enhancements High Profile: 188 controls, 182 control enhancements Privacy Profile: 75 controls, 21 control enhancements
CIS Controls v8 safeguards	18 controls containing 153 safeguards Implementation Group 1: 56 safeguards Implementation Group 2: 130 safeguards Implementation Group 3: 153 safeguards
ISO/IEC 27002	4 clauses containing 93 controls (in the previous 2013 version, 14 clauses containing 114 controls)
Katakri	42 criteria items containing 122 requirements Restricted Level: 89 requirements Confidential Level: 103 requirements Secret Level: 109 requirements
Julkri	83 criteria and 139 sub-criteria Minimum Subset: 50 essential, 47 optional Maximum Subset: 222 essential

of 298 controls and 709 control enhancements. From a prioritization point of view, even with a low profile, it already contains 131 controls and 18 control enhancements, which is more controls than ISO/IEC 27002 contains in total. This can be explained with the control specification, where SP 800-53 controls are more atomic, whereas ISO/IEC 27002 controls contain more broader definitions, as the cross-references in the NIST SP 800-53 document indicate. Therefore, SP 800-53 seems to be more applicable to situations where small subsets of controls are prioritized for different use cases.

However, all of the catalogs presented, excluding Julkri, have a fairly large number of controls even at the initial level. Even the lowest percentage of CIS Controls includes 36% all safeguards in the first implementation phase. Therefore, prioritization focuses on the least critical controls, where more than a third of the controls are counted as the highest priority controls. As mentioned previously, many organizations struggle with implementation with basic controls. Therefore, prioritization should be taken into account even in the most critical controls.

2.6 SME challenges in information security

Limited resources have been consistently identified as the most critical constraints to invest to information security [2, 37]. In particular, the lack of financial resources

has been identified as the most critical issue preventing SMEs from managing information security risks [37]. The irregular revenue streams of SMEs also affect IT security investments [37]. Decision-making on security investments also depends on understanding the threat, organizational behavior, and awareness of available countermeasures. Increasing awareness of information and cyber security at the managerial level of SMEs supports security investments [2]. Usually in SMEs, decision makers in the organization have several roles, which can lead to biased decisions when considering, for example, supply chain security when selecting potential contractors or service providers [2]. Where most large companies review cyber risks from their suppliers, this activity is much less common for SMEs, leading to increased supply chain risks [18].

SMEs often lack the input data necessary quantitative risk assessment models [13]. Lack of input data can lead to incorrect risk assessment results, again leading to incorrect security investments. Information security risk management is not trivial, as even security professionals can get different results [79]. Especially small companies do not have the financial possibility to have a hired security professionals but need to rely on external support or their own limited competence. As medium sized companies tend to outsource IT security management more than small companies, outsourcing can also lead to knowledge gaps in which security measures are being implemented to protect the business [17].

In SMEs, technical information and cyber security controls are often managed by IT personnel, who need to perform other tasks [17]. SMEs also have difficulty implementing the selected security controls correctly or implementation is not optimal [2]. Although the technological evolution of machine learning and artificial intelligence introduces new controls and strengthens existing technical security controls, it is not clear that such advances will be widely used by SMEs before the cost of the technology is reduced [83].

Organizational behavior and culture have an impact on security investments and decision-making. In SMEs, employees attitudes have a negative impact on the management decision making to implement new security solutions. Also, lack of cybersecurity knowledge and awareness of employees causes low motivation to improve the cybersecurity posture of SMEs [37].

3 RESEARCH METHOD

This chapter represents design science research method and how it has been used in the information and cyber-security research. The chapter also describes the role of design knowledge in security risk management and how design science research uses existing knowledge as a foundation and contributes new knowledge as result of the research.

3.1 Design science research

Design science research aims to develop and evaluate innovative artifacts or systems to address identified problems, emphasizing both the creation and the utility of these solutions [41]. Its primary objectives are to advance knowledge through the design and evaluation of practical solutions and to contribute to the improvement of real-world practices or environments [70]. Venable and Baskerville [92] define DSR as *“research that invents a new purposeful artefact to address a generalised type of problem and evaluates its utility for solving problems of that type.”* Hevner [39] constructed three cycles to describe the DSR process represented in Figure 5.

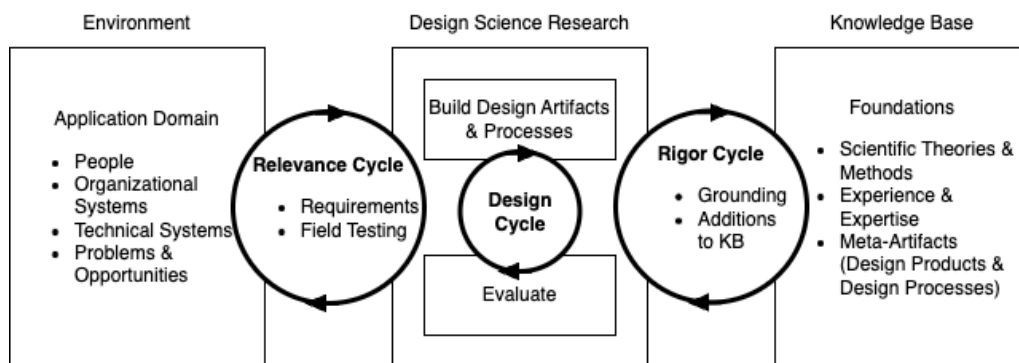


FIGURE 5 Design science research cycles by Hevner [39]

The DSR cycles are as follows [40]:

1. the relevance cycle,
2. the rigor cycle, and
3. the design cycle.

The relevance cycle initiates design science research with an application context setting the requirements for the research as input and receiving developed artifacts to be evaluated in field tests as output. The relevance cycle can be repeated to complement requirements and collect feedback from new field testing iterations. The results of field testing will indicate are additional relevance cycles needed in DSR project. Field testing may also point out that the original requirements for research have been incorrect or incomplete, with the result of an artifact satisfying the requirements but still inadequate to respond to the initial problem [40]. Hence, the relevance cycle is important not only for verifying produced artifacts but also to verify that the defined requirements and evaluation criteria for the artifacts meet research goals.

Where the relevance cycle binds design science research to practice, the rigor cycle provides experiences and expertise that define the state-of-the-art as well as existing artifacts in the application domain of the research [40]. The rigor cycle uses the known design processes and the known relevant design artifacts to guarantee the innovativeness of the research project. When comparing a DSR project with a generic IT system development project, the rigor cycle is what differentiates a DSR project utilizing scientific theories that can be combined to a creative design. The rigor cycle also includes the risk of utilizing inappropriate theories, which may lead to limited development of the artifacts.

Between the relevance and rigor cycles, the internal design cycle is the heart of any DSR project. The research activities in this cycle alternate between constructing and evaluating the artifact, followed by feedback to enhance the design. A design cycle must maintain the balance between construction and evaluation of the evolving design artifact. The design cycle consists of multiple internal iterations of development and testing before the contributions are outputted to the relevance and rigor cycles [40].

Peppers et al. [70] also presented a more refined composition of the DSR steps as follows:

- Step 1. Problem identification,
- Step 2. Definition of solution objectives,
- Step 3. Design and development,
- Step 4. Demonstration,
- Step 5. Evaluation, and
- Step 6. Communication.

Although the steps are presented in sequential order, the process may actually start from any of Steps 1-4 and then move outward. For example, objective-centered research could start from Step 2, and design- and development-centered research would start with Step 3 [70]. In the evaluation phase, a commonly used assessment criterion for a DSR work consists of the following elements [91]:

- Relevance of the problem to industry/society clearly established
- Significance of the problem to industry/society clearly established
- Depth of analysis and clarity of understanding of the problem and its causes
- Depth or profoundness of insight leading to the new design artifact
- Novelty of the new design artifact
- Size and complexity of the new design artifact
- Amount of effort that went into the development of the new design artifact(s)
- Elegance of the design of the new artifact(s)
- Simplicity of the design of the new artifact(s)
- Clear understanding of why the new artifact works

Depending on when the DSR artifact is evaluated, ex ante and ex post evaluations are distinguished. Ex ante evaluations are performed before artifact instantiation, while ex post evaluations occur after artifact instantiation [93].

3.2 Knowledge in security risk management

DSR aims to generate knowledge about how artifacts can and should be constructed or designed to achieve a desired set of goals, called design knowledge (DK) [9]. DK includes information on the important problem, the designed solution, and the evaluation, which are conceptualized in Figure 6.

The DK produced in a DSR project can be richly multifaceted [9]. In DSR projects, two forms of knowledge are created: descriptive knowledge (denoted Ω , or omega) and prescriptive knowledge (denoted λ , or lambda). Descriptive knowledge, or Ω -knowledge refers to the "what" knowledge concerning natural phenomena and the principles and patterns among these phenomena, and prescriptive λ -knowledge is the "how" knowledge of human-built artifacts [35]. DSR projects typically contribute to the λ knowledge base by providing new insights into technological advancements that directly affect individuals, organizations, or society while also allowing the development of future innovations.

The λ -knowledge has two subcategories. The new knowledge of the design theories related to these solutions is collected in the Solution Design Theories

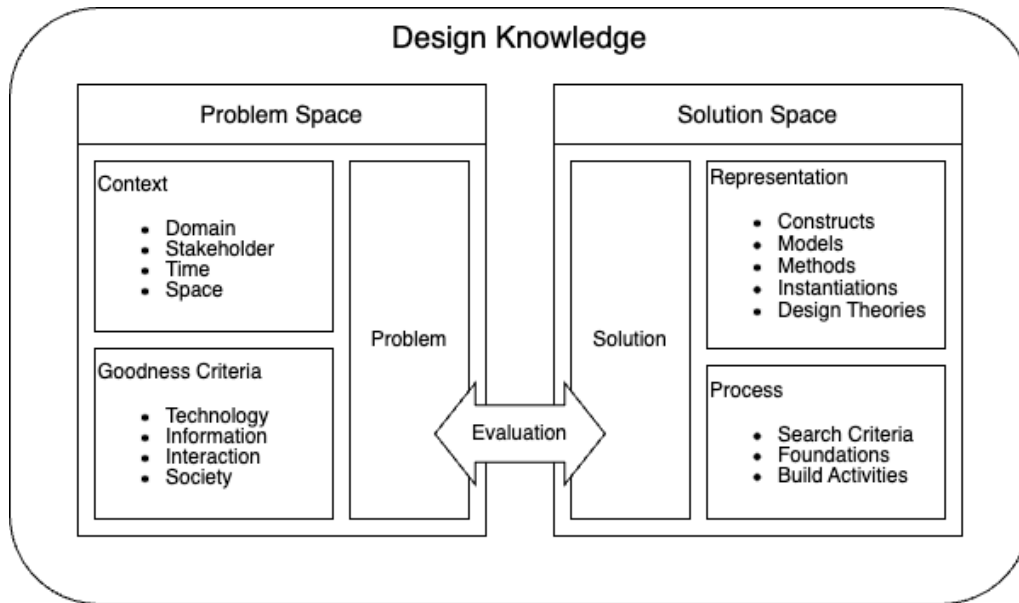


FIGURE 6 Components of design knowledge for a specific DSR project [9]

knowledge base. Solution Design Entities collect prescriptive knowledge as represented in tangible artifacts, systems, and processes designed and applied in the problem solution space [35].

Figure 7 contains six arrows, which correspond to six design theorizing modes. Each of them indicates the different knowledge types, either by using the knowledge in a DSR project to produce project design knowledge or by contributing selected knowledge back to a distinct part of the knowledge bases. It is also possible that an actual knowledge contribution draws on more than one mode at a time. The theorizing modes are as follows:

1. Ω -knowledge enhances the comprehension of a problem, its context, or the design of a solution entity.
2. The design and real-world application of solution entities or knowledge improve our understanding of the world.
3. The solution design knowledge informs the design of a solution entity, a design process, or a design system.
4. The effective principles, features, actions, or effects of a solution entity or a design process or system are abstracted and documented in the solution design knowledge.
5. Previously effective solution entities, design processes, or design systems are reused for or inform future designs of new entities, processes, or systems.
6. Effective solution entities, design processes or design systems contribute to λ -knowledge.

The design theorizing modes presented emphasize the different knowledge contributions that a DSR project can make to Ω and λ [24]. Theorizing modes are later utilized in the presentation of research contributions of this research.

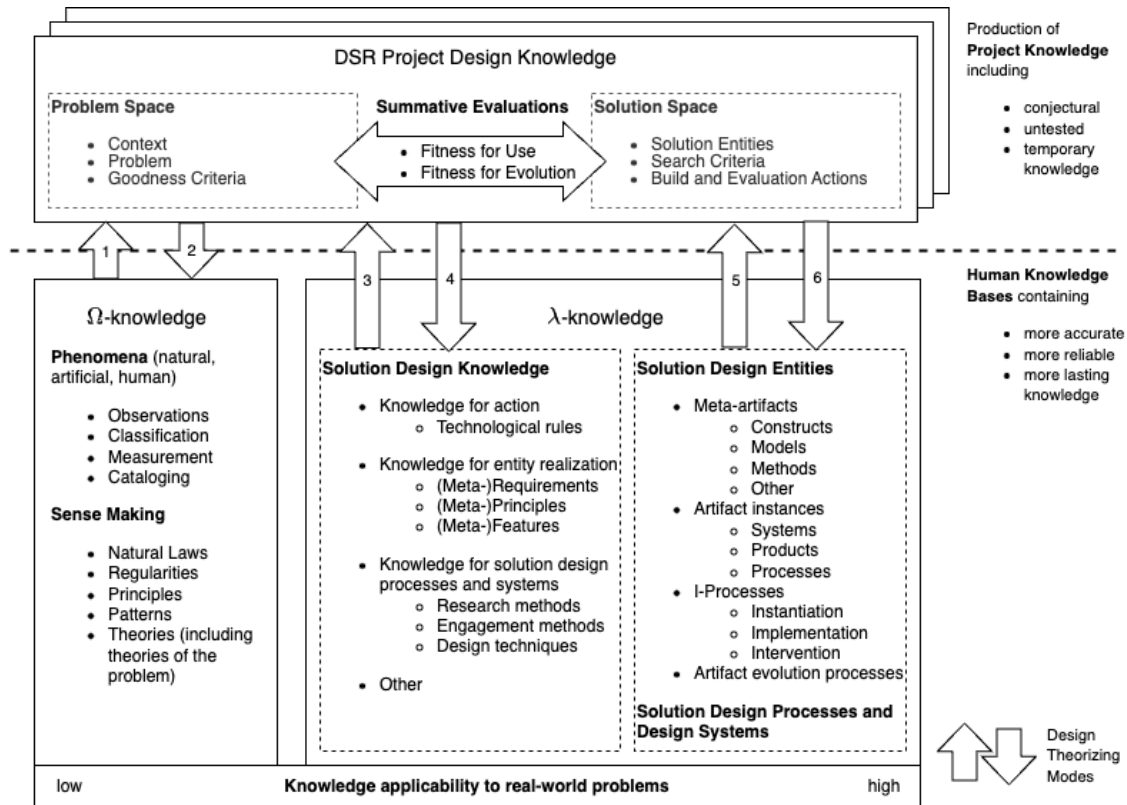


FIGURE 7 Knowledge utilization, production, and contribution to DSR [24]

3.3 DSR in information and cyber-security research

As shown, there is no information systems research that is domain specific in general on the DSR. However, considering the widespread usage of DSRM in information systems research, there has been a relatively limited number of publications in which it has been used in information and cyber-security research.

In the domain of information and cyber-security management and governance, DSR has been used in the development of the national cyber-security framework [22], the development of the resilience governance framework and design aspects for resilient cyber-physical eHealth systems [74], and the development of information security governance recommendations and road maps [96]. DSR has been used in the development of a privacy impact assessment methodology [67] and a framework for assessing the privacy impact of maritime surveillance systems [73]. Govender et al. [33] have used DSRM in the development and evaluation of an information security assessment tool. DSR has been used in the development of technical artifacts in cyber-threat detection and threat communication artifacts [26] and in the generic framework for the continuous monitoring and benchmarking of the cyber-security status of an organization [57].

There are multiple publications in which DSR has been used in the development of information and cyber-security competence and cultural artifacts, including the definition of requirements for cyber-security training platforms [38], the conceptual framework for increasing cyber security in higher education insti-

tutions [3], and the gamification and development of information security training [82]. It has also been used in the SME context in the development of the model to present the artifacts of an IS security culture and to verify the model in the SME context [45]. As the presented publications show, the focus of DSRM research in the information and cyber-security domain has been more on artifact development than on developing DSR practices for information and cyber-security research, which highlights the potential research gap in the area.

3.4 Knowledge-intensive business processes

Modern information-driven work involves knowledge workers using their distinguished skills, experiences, and expertise to cope with sophisticated and non-routine tasks. These processes are called knowledge-intensive business processes (KIBP) [65]. Although there is no unambiguous definition of which processes are KIBP, the characteristics of KIBP include creativity, eligibility for automation, and level of complexity [44]. Information security risk management is KIBP, as it is not only based on professional knowledge but also serves as a critical source of information for an organization. KIBP are utilized in knowledge-intensive business services (KIBS). The characteristics of KIBS include that they rely heavily on professional knowledge or are themselves primary sources of information and knowledge. Mundbrod and Reichert [65] have discerned eight challenges that KIBP should address:

1. Meta-model design: creation of a meta-model that accommodates necessary information and activities.
2. Life cycle support: KIBPs require flexibility during both the design and run-time phases.
3. Variability support: the results of KIBP are significantly influenced by the knowledge applied during the process, which requires a high degree of variability.
4. Context support: in relation to lifecycle and variability support, KIBPs can be highly tailored to particular contexts, necessitating the inclusion of contextual parameters.
5. View support: when there is a large volume of activities and knowledge needed for process conduction and execution, the need for personalized views arises.
6. Authorization support: authorization support is essential from a security standpoint, as the execution of KIBPs involves a diverse set of tasks and information, necessitating collaboration among individuals in different roles.
7. Synchronization support: for tasks to be executed successfully, it is crucial that all required information is available in a timely manner.

8. Integration support: KIBPs can directly interact with and trigger predefined and standardized business processes. Therefore, integration is necessary to obtain status updates and the results of these processes.

The challenges presented can also be applied to the information and cyber-security risk management process and the systems that support the process.

4 SUPPORTING SECURITY CONTROL SELECTION

The included articles are divided into three pairs following the structure of the research in the sequence of background, development, and analysis. The first two articles focus on analyzing the existing security controls catalogs at the time of publication and provide background information required in the following articles. These articles provide the knowledge about problem space and existing solutions at the time. The second pair of articles, Articles III and IV, represent the development of the SMW-based artifact to support security control selection and information security risk management. From the DK point of view, these articles focus on the development of artifacts in the solution space. The last pair of articles analyzes the process and produced artifacts on the DSR point of view. In detail, Article V analyzes the development of SMW-based artifacts from the DSR perspective, and Article VI evaluates Julkri development using DSR principles as Julkri development takes into use results of Articles III-V.

The articles are included in chronological order. Nonetheless, it should be noted that the timeline of the articles is reasonably long. Therefore, the versions of Katakri and ISO/IEC 27001 and 27002 in Articles I and II were already updated twice before the publication of Article VI.

4.1 Security control semantics

4.1.1 Article I: Information security management system standards: A gap analysis of the risk management in ISO 27001 and KATAKRI

Nykänen, R., & Hakuli, M. Information security management system standards: A gap analysis of the risk management in ISO 27001 and KATAKRI. In Proceedings of the 12th European Conference on Information Warfare and Security (Vol. 1, pp. 344-350). 2013.

Research aims

The aim of this article was to evaluate the risk management requirements of two different information security management specifications. The article analyzes differences and gaps in information security risk management requirements between these two approaches.

Data and methods

The analysis included a comparison of the widely used international ISO/IEC 27001:2005 Standard and the Finnish national Katakri Version II. Both specifications were at the time of analysis the latest versions of the specifications, but have since been updated. The risk management process requirements of ISO/IEC 27001 have not changed significantly in the newer versions although the Plan-Do-Check-Act cycle has been removed. However, Katakri and its content have evolved more structurally in newer versions.

Main results

The results of the analysis indicate some gaps in the requirements of the information security risk management process between these two specifications, though the general requirements are similar. Minor deviations include, for example, triggers of a risk assessment process and management approval of implemented controls. Both frameworks follow a common information security risk management process, which is defined in more detail in ISO/IEC 27005 [47].

Research contributions

Although security risk management requirements have minor deviations between ISO/IEC 27001 and Katakri, the requirements are analogical at the general level. Additionally, there was no notable variation in requirements based on organizational differences. In Katakri, risk management requirements were similar regardless of the security classification of information. Based on the findings, a research gap was identified to evaluate specifications from the security control perspective, which was conducted in Article II.

4.1.2 Article II: Comparison of Two Specifications to Fulfill Security Control Objectives

Nykänen, R. & Kärkkäinen, T. Comparison of two specifications to fulfill security control objectives. In the 13th European Conference on Cyber Warfare and Security, ECCWS-2014 (p. 150). 2013 Academic Conferences International Limited.

Research aims

The objective of the research was to analyze the security controls of Katakri Version II and the ISO/IEC 27002:2013 controls specification in continuation of the comparison of risk management requirements conducted in Article I.

Data and methods

Research was conducted analyzing both structural and content differences of Katakri Version II to ISO/IEC 27001:2013 and 27002:2013. As ISMS requirements are specified in ISO/IEC 27001 and security controls in ISO/IEC 27002, a comparison was conducted to combine these two standards as Katakri contains both requirements in one specification.

Main results

Both specifications contain an exhaustive set of information security controls to protect the assets of organizations. The comparison results indicate that although the security controls in both specifications are mostly similar, there are controls and concepts that exist only in either of the specifications. For complementary controls, it is typical that these controls are specific to a particular use case, but not common to all organizations. An example of such a control is the TEMPEST countermeasures required by Katakri to protect information at the highest levels of national security classification. Other Katakri complements to ISO/IEC 27002 controls include specific national requirements for the recruitment process, such as the use of drug tests and probationary periods used in recruitment, which may not be allowed in the recruitment process in all countries.

Complementing controls from ISO/IEC 27002 include, for example, controls related to information systems development, the reporting of security incidents, and the gathering evidence in case of security incidents. It should be noted that many of the differences in Katakri Version II and the ISO/IEC 27002:2013 version have been changed in the later versions of both specifications.

The results also show that there is no common taxonomy for information security requirements and security assessments. The lack of a common vocabulary is not supporting the usage of the specifications, especially in the case of nonprofessional users.

Research contributions

As a conclusion of the comparison, both analyzed specifications mostly include overlapping security controls. However, there are also complementary areas. The results also highlighted the limited prioritization of control in both specifications, which would especially help SMEs or other organizations with limited resources and security competence. In Katakri, controls were prioritized based on the information confidentiality classification. In ISO/IEC 27002:2013, there was no prioritization of controls or attributes to limit or search controls. Based on the

findings, the development of an enhanced security control catalog was started to develop new artifacts to support security control selection and the security development road map-type of approach.

It should be noted that the OSCAL framework was introduced since the publication of Article II and has provided the common taxonomy and vocabulary for the definition of security requirements and assessments. However, the OSCAL framework has been adopted only by the NIST standards and frameworks.

4.2 Enhanced control catalog

4.2.1 Article III: Tailorable Representation of Security Control Catalog on Semantic Wiki

Nykänen, R., Kärkkäinen, T. (2018). Tailorable representation of security control catalog on the semantic Wiki. In: Lehto, M., Neittaanmäki, P. (eds) *Cyber Security: Power and Technology. Intelligent Systems, Control, and Automation: Science and Engineering*, vol. 93. Springer, Cham.
https://doi.org/10.1007/978-3-319-75307-2_10

Research aims

The article evaluates the adequacy of the semantic wiki as a security control catalog platform to build an information security knowledge base that would especially help SMEs develop and maintain their security postures. At the time of the research, security control specifications, such as ISO/IEC 27002 and NIST SP 800-53, were mainly published as documents. NIST SP 800-53 was also available as a website where controls could be filtered based on the security baseline and family, though no advanced functions were available to find potential controls. Therefore, the objective of the research was to analyze how a wiki platform could be used to introduce advanced features.

Data and methods

Research represents the first design iteration of the development of the DSR artifact. MediaWiki, the platform used by Wikipedia, with the Semantic MediaWiki (SMW) extension was selected to be the platform. As standard MediaWiki limited features to define structural elements for the wiki, SMW adds semantic annotations to enable structural elements on wiki pages and, for example, advanced search functions.

The process of developing the initial artifact can be summarized in the following steps:

1. Analysis of the NIST SP 800-53 structural model.
2. Mapping of the model to semantic wiki concepts.

3. Building transformations to create structured documents from NIST SP 800-53 content that was imported into a wiki.
4. Validation of the semantic model and transformation results.
5. Definition of additional views of data using semantic wiki features.

NIST SP 800-53 was selected to be used as an initial control catalog, as it was publicly available in XML format free of charge. NIST SP 800-53 has one of the highest number of security controls and control enhancements, which would allow a better evaluation of performance of a platform with a large data set.

Main results

As a key result, it was demonstrated that the SMW can be used as the basis for creating a common security knowledge base ontology for an information security knowledge management system. Although there were some issues with data structures, all of them can be resolved with minor adjustments.

As a constraint, the created ontology is based on only one specification, and hence, it does not provide a universal security control catalog ontology, but represents common elements of security control semantics. However, no limitations were detected to extend the object model to support multiple or combined security control catalogs, although some issues, such as the unique page naming constraint, need to be addressed in the object model.

The implemented SMW instance also provided the possibility of utilizing a semantic search to gather the statistics of the control catalog. A semantic search also enabled the analysis of internal relationships of security controls better than document or Excel spreadsheet presentations. For example, controls having a high number of references from other controls can be seen as more fundamental, which would increase their implementation priority.

Research contributions

This research iteration was important to verify that SMW can be used as a platform for the enhanced security control catalog. The article lists a number of potential enhancements, which are considered in the second design iteration. As the article introduced the initial version of the artifact, the following article, Article IV, implemented additional functions to support common risk management functions and to support control selections.

4.2.2 Article IV: Supporting Cyber Resilience with Semantic Wiki

Nykänen, R., & Kärkkäinen, T. Supporting cyber resilience with semantic wiki. In Proceedings of the 12th International Symposium on Open Collaboration (pp. 1-8). 2016.

Research aims

The article presents the second iteration of the design of the SMW-based platform to manage information security in organizations. The objective was to create an initial version of a security control catalog and extend it with security risk management functions.

Data and methods

The research utilized DSR to create an enhanced security control catalog to support organizations' in risk management actions. The artifact presented in Article III was used as a baseline for further development. The article analyses the artifact against six common information security risk management challenges [29]:

1. To establish an asset and control inventory.
2. To assign values to assets.
3. To predict the risks correctly.
4. To avoid overconfidence on the ISMS.
5. To share knowledge.
6. To balance the risk vs. cost trade-offs.

New functionality and schema additions were introduced to respond to the challenges presented.

Main results

In the second iteration of the design, additional functions were introduced to the security control catalog combined with the knowledge management system as a design artifact. A semantic MediaWiki-based approach also allows one to manage information security risk knowledge within organizations. We utilized the Semantic MediaWiki platform as it supports the structured content required for the formal presentation of a control catalog, but can be adapted to an organization's specific needs for knowledge management systems better than domain-specific applications.

Semantic MediaWiki supports a feature called page templates, which create a specific structure for a wiki page. In the demonstration, a number of new page templates were defined for the structural elements of risk management concepts. In addition, a semantic search was used after the initial version to create features to browse the control catalog and find relevant controls.

The metamodel was extended with the risk taxonomy based on the taxonomy defined by Cebula et al. [10]. The security control and control enhancement were enhanced with CIA properties to allow for select suitable controls based on information security properties, as well as to have statistics based on the properties.

Research contributions

The article presented a second design iteration to create a wiki-based representation of the security control catalog to support risk management activities, especially the selection of security controls. The artifact created indicated that SMW can be used as the foundation for creating functions to support organizations' in security risk management tasks.

In response to the presented risk management challenges, the prototype was found to partially solve the problems, especially with knowledge sharing, and the proposed approach increased the overall understanding of risks and their relationships.

The results also indicate that there are multiple potential ways to support the selection of security controls using different types of attributes and semantic searches. Moreover, the lack of an asset inventory was seen as a deficiency as risks or controls could not be linked to assets.

4.3 Evaluation of artifacts

4.3.1 Article V: Knowledge Interface System for Information and Cyber Security Using Semantic Wiki

Nykänen, R., & Kärkkäinen, T. A knowledge interface system for information and cyber security using semantic wiki. In S. Chatterjee, K. Dutta, & R. P. Sundarraj (Eds.), *DESRIST 2018: Designing for a Digital and Globalized World: 13th International Conference* (pp. 316-330). 2018. Springer International Publishing. Lecture Notes in Computer Science.

https://doi.org/10.1007/978-3-319-91800-6_21

Research aims

This article presented the evaluation of how to use design science research to assess the knowledge base of information security. As DSR has been used merely in information system research projects, it is beneficial to analyze in detail which of the DSR evaluation approaches are valid for different types of compliance criteria that also include standards and other specifications.

Data and methods

To evaluate our artifact, the criteria for assessing DSR work by Venable [91] is used. Furthermore, the SMW platform to support information security risk management was identified as an instance of KIBS, and therefore, the second objective of the research was to analyze artifacts as a KIBS instance. The article evaluates the artifacts according to the eight KIBP challenges presented in [65]. The data used in the artifact's development are the same as in Article IV, with minor enhancements

to the SMW platform.

Main results

The DSR process is composed of three related cycles: i) the relevance cycle, ii) the rigor cycle, and iii) the design cycle [40]. The three cycles and outcomes in the research are presented in the Figure 8. The relevance cycle ensures that technology-based solutions solve important and relevant business problems. The relevance cycle of the research was based on the prior research in Articles I and II. The rigor cycle provides the prior knowledge as a foundation for research [43], where the research utilized common risk management processes and the NIST SP 800-53 security controls specification. The design cycle contributed to the construction of the SMW instances and evaluation of the artifact.

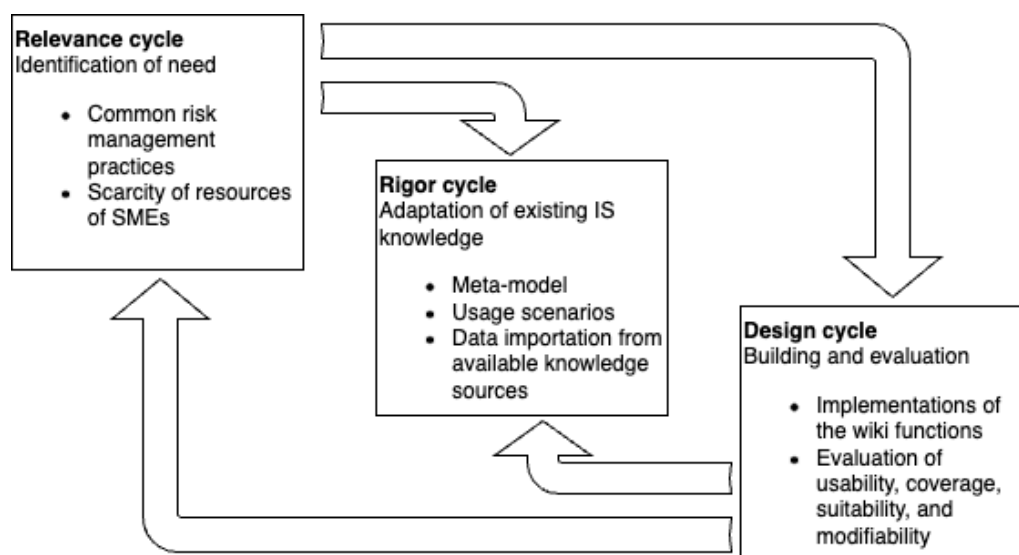


FIGURE 8 DSR cycles with outcomes

From an artifact life cycle point of view, the KIBP evaluation indicated that the created artifact required further development if it were to be provided to SMEs as a risk management platform. Where single instances of the SMW-based wiki are easy to deploy for an IT professional, for SMEs without sufficient IT competence, it would be an unobtainable task. As this would also be the target audience of the tool, the service delivery model should be developed further and should be taken into account in the meta-model of service.

Research contributions

The results indicate that the artifact developed in Articles III and IV satisfies the criteria for DSR work. The evaluation of the artifacts as KIBP show weaknesses in service delivery, which has been excluded from the design. The identified weaknesses should be addressed in case of commercializing the enhanced control catalog to a product, but are outside of the scope of this research.

4.3.2 Article VI: Analysis of the Next Evolution of Security Audit Criteria

Nykänen R., Kelo T., and Kärkkäinen T. Analysis of the next evolution of security audit criteria. *Journal of Information Warfare*, vol. 22, issue 4, pp. 25-39, 2023.

Research aims

The focus of the article was to evaluate the development of the Julkri criteria [6] and if the Julkri criteria provide enhancements compared to existing security control catalogs.

Data and methods

The research utilized the Framework for Evaluation in Design Science (FEDS) [93] to evaluate Julkri as a DSR artifact. The FEDS evaluation episodes were derived from the evaluation principles of a security audit criteria of Kelo et al. [56]. The evaluation principles include the design, implementation, and utilization of security audit criteria. Some of the utilization phase principles were outside of the scope of the Julkri development project and were, therefore, ignored in the evaluation.

Main results

The research results indicate that security audit criteria and security control selection can benefit from a use case-driven approach where an applied subset of security controls is selected from an exhaustive list of security controls. Figure 4 represents the process by which effective criteria are selected in Julkri. The number of essential and optional security controls adapts to security goals based on preconditions. Additionally, enhancing the meta-models of existing control catalogs with new features can support catalog users in their control selection and efficient utilization of the risk-based approach.

Other results indicate that the use of an existing control catalog is a good starting point for the development of the new audit criteria. As comprehensive security control catalogs exist, the process should merely consider if updating and validating the coverage of the catalog is sufficient. The development of technologies used by organizations needs to be addressed when updating security control catalogs, which was noticed when the draft version of Julkri was published for commentary. In the case, the feedback concerned how requirements adapt to the services using the zero trust principle instead of traditional network perimeter protection. This highlights the principle that security control catalogs and security requirement specifications should focus on the objective and not the implementation. Implementation options can be provided as support information, but not as requirements, for example, in the case of security awareness versus security training.

Research contributions

Julkri utilizes multiple aspects of control selection from the results of the previous Articles IV and V. Julkri had also focused on supporting differently sized public sector organizations with different resource levels. The article also includes the structural analysis of four security control catalogs, including their recent advancements. In the analysis, it is shown that some of the enhancements presented in Article IV have been implemented in ISO/IEC 27002 in the recent update.

The development of Julkri also indicates that expert knowledge can be used to define security control sets for specific use cases, which will reduce the competence requirements of organizations using the security control catalogs. As use case and other preconditions can be used to filter and prioritize security control implementation, organizations can more efficiently focus on security control implementation instead of assessing the feasibility of different security controls and their implementation options.

Julkri, which was initially not developed as a design science research, aligns with the characteristics of the DSR artifact according to its outcomes. In addition, results indicate that the security control catalog or security audit criteria can be evaluated according to DSR principles complemented with domain-specific evaluation criteria. However, if Julkri would have been evaluated during the development phase utilizing the FEDS framework [93], different evaluation strategies could have been considered in addition to the simple evaluation strategy, which was found to be the most suitable for summative ex-post evaluation. In summary, when defining the evaluation criteria for information and cyber-security DSR artifacts, the following considerations should be taken: i) DSR evaluation strategy, ii) generic DSR evaluation criteria, and iii) domain-specific evaluation criteria.

5 DERIVED ARTIFACTS

This chapter presents derived artifacts that are generalized and developed further from the artifacts presented in the included articles. The chapter also contains an aggregation of the DSR artifacts created in the research to summarize the research results.

5.1 Risk assessment process utilizing an enhanced control catalog

The combined object model consists of a security control catalog with generic information and an organizational security knowledge base. The knowledge base initially contains generic enhanced security control catalog. When an organization starts use the knowledge base, the organizational information including security goals and control implementation status is collected to the knowledge base. Later on this information is used to prioritize the control implementation suggestion to the organization. Figure 9 describes a process to utilize the knowledge base and the control catalog in combination with organizational information.

As in the first place, the organization shall define preconditions, similar to Julkri. Using the complete object model, the selection shall also include attributes such as asset types owned by the organization and potentially identified threats. From a user's point of view, this phase includes the setting of security objectives and the identification of organizational assets at a high level. Based on preconditions and control catalog information, controls are scored, and a prioritized set of controls is proposed to the organization. In this phase, the user should be able to filter out controls that are irrelevant or out of scope for the organization. An organization should be able to provide a control implementation status if a proposed control is already implemented or is infeasible to implement. When an organization implements the control, the knowledge of the implementation status and details should be recorded in the organizational knowledge base.

As in risk management in general, the process is expected to be continuous and iterative. An organization should re-evaluate preconditions on a regular

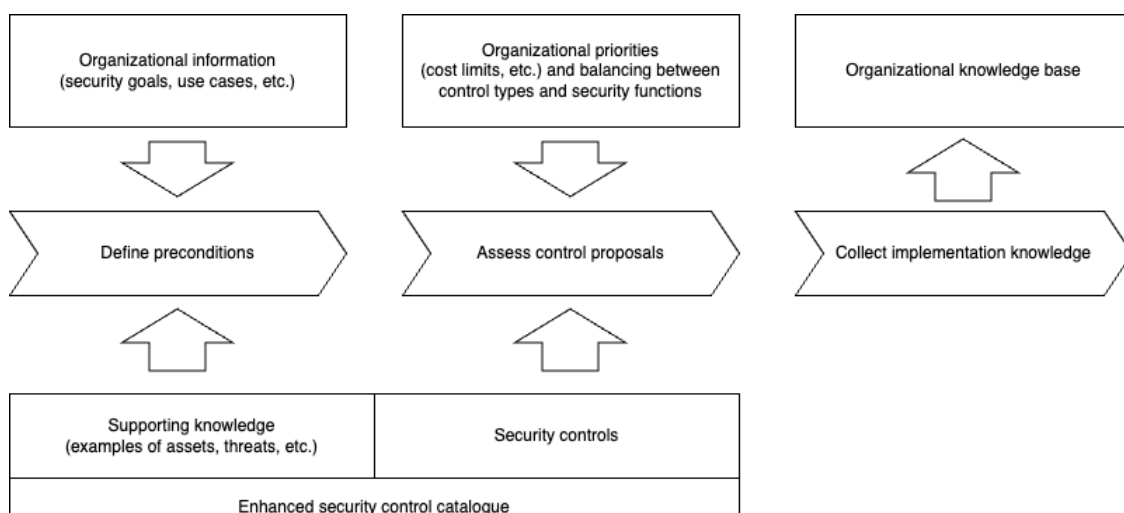


FIGURE 9 Proposed process to utilize the knowledge base and the enhanced control catalogue

basis to identify potential changes in the proposed actions. Moreover, the implementation status of the controls should be reflected in the proposed control list.

5.2 Control catalog object model

To support the presented process, an enhanced control catalog metamodel is required, as current control catalog metamodels do not support the required semantics. The artifacts presented in Articles III-VI, including Julkri criteria, all contain subsets of a proposed security control meta-model. However, the presented model is not included as a whole in the articles.

The core of the enhanced control catalog object model is presented in Figure 10 in UML notation. The core of the model is adapted from the OSCAL schema, where security control and control enhancement combine to form a two-level hierarchy for controls. This also enables the use of NIST SP 800-53 controls as a basis for the control catalog. Controls and control enhancements are categorized using control families. The security controls have a two-level approach, where control enhancements as sub-elements of a control can refine. This allows the control definitions to be more atomic rather than consisting of long descriptions. Security control and control enhancement have identical structures, excluding the parent reference to security control in control enhancement.

Security control implementation cost estimates do not exist in any of the current control catalogs at present. However, from a quantitative risk management point of view, the cost of control implementation is one of the key attributes, to distinguish which controls are feasible for implementation in the organization and which are not. The meta-model supports the definition of initial and recurring annual running costs of security controls. This knowledge allows organizations

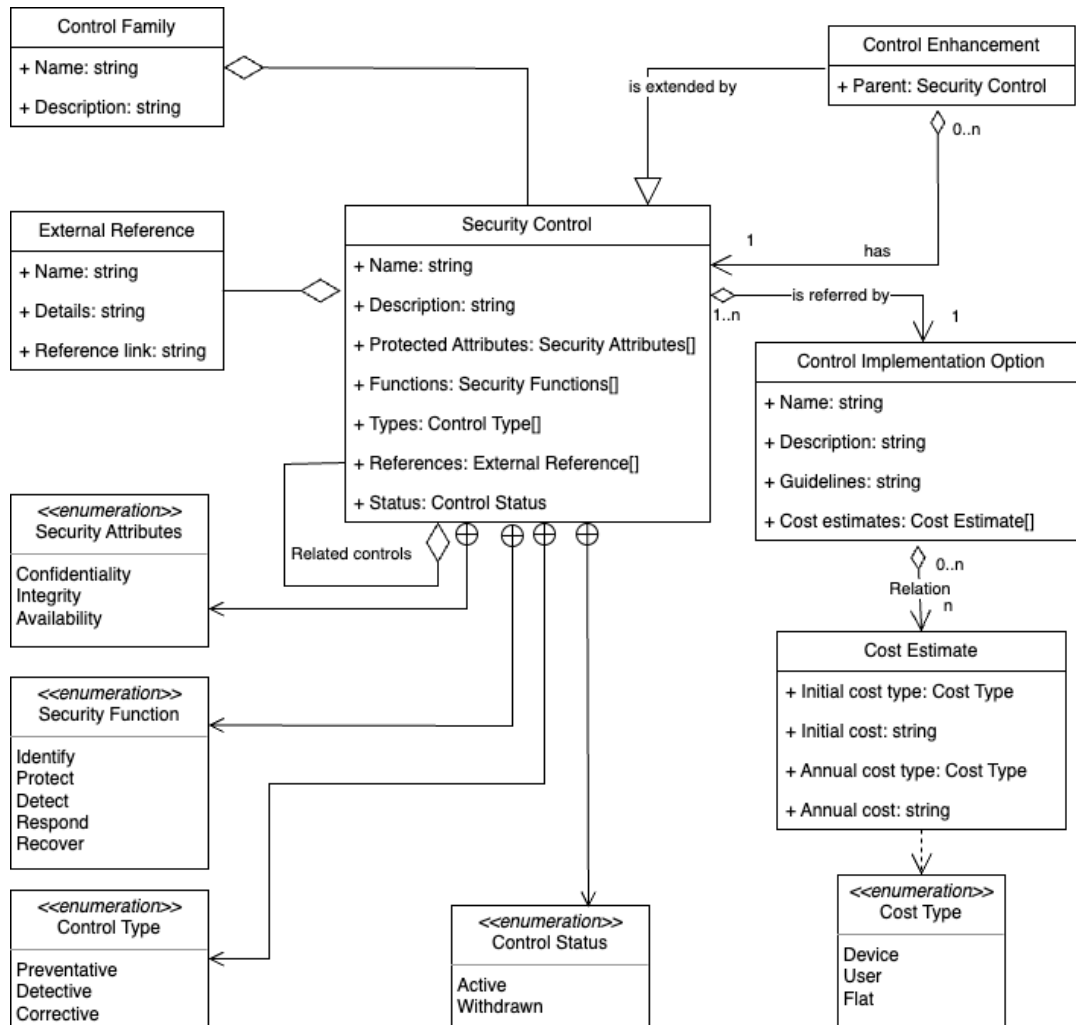


FIGURE 10 Core meta-model of the enhanced control catalogue

to have an initial estimate of the potential costs of the control implementation. It also allows SMEs with limited budgets to rule out the security controls that have a high initial investment cost, which advanced technical solutions typically do.

The control implementation option also contains detailed guidelines. The lack of detailed guidelines to implement security controls has been identified as one of the challenges in information and cyber security for SMEs [78]. The security control versioning is excluded from the metamodel for simplification, though it contains the control status attribute, as NIST SP 800-53 retains the identifier of retired controls to avoid conflicts between versions. However, the meta-model can be enhanced to support control versions. As the presented core of the meta-model only supports simple control filtering, next previously unpublished additions to the control scoring model are presented the next.

5.3 Control scoring model

In addition to the combined presented process and aggregated models, a design iteration has been executed to enhance the control selection from a multi-criteria decision-making point of view. The results of this design iteration are not included in the presented articles but provide an additional artifact of the research.

To support the prioritization and selection of security controls, all security controls are scored based on preconditions provided by the user. In Julkri, control prioritization was implemented using simple rule-based logic, but similar results could have been achieved with the scoring approach. This approach will calculate a priority score for each control based on the preconditions defined by the user. Figure 11 represents the UML model for the essential elements for control scoring. The classes presented complement the UML model of the previous control catalog in Figure 10.

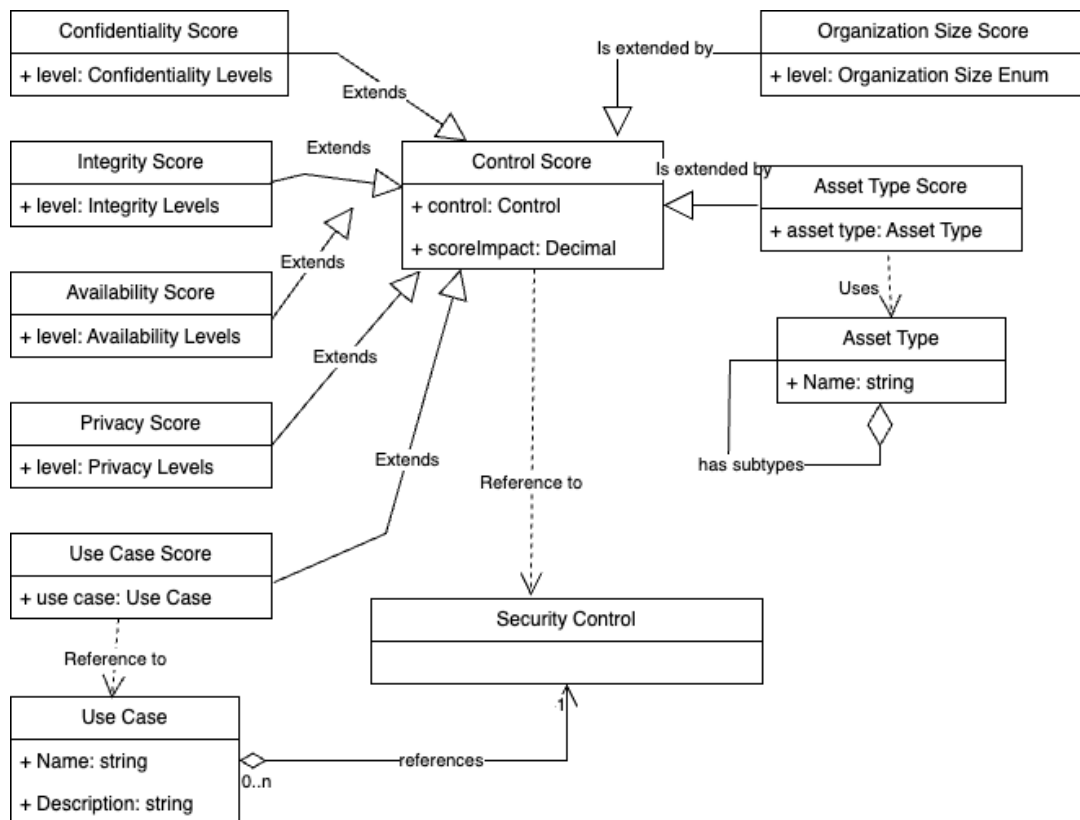


FIGURE 11 Control scoring classes

The Control Score is an abstract base class that is inherited by the scored attribute class instances. Each scoring class refers to a security control or a control enhancement. Each scoring class also has a numeric score impact. The scoring classes with explanations are presented in Table 5.

The object model does not include the definitions of the CIA property scales, which are typed into the UML model Confidentiality, Integrity, and Availability Levels. As mentioned, Julkri used the confidentiality scale derived from Finnish

TABLE 5 Scoring class explanations

Scoring class	Description
Confidentiality, integrity, and availability scores	Confidentiality, integrity, and availability levels should correspond to the organizational priority of information security properties.
Privacy score	Privacy levels should correspond to the levels of personal data that the organization is processing. In EU, this should reflect the two levels of personal data defined in the GDPR.
Use case score	The use case score reflects the control importance in the specific use case.
Organization size score	The size of the organization has an impact on the feasibility of certain controls. If certain controls should be favored for specific organization sizes, Organization Size Score values should reflect those priorities.
Asset type score	Different controls are suitable for different asset types. The asset type score shall emphasize the suitable assets for specific asset types. When the organization selects in the preconditions the asset types it has, the score shall prioritize relevant controls.

national information security classification levels. At any rate, such an approach is not suitable for a control catalog intended to be used by all kinds of organizations. For confidentiality, integrity, and availability, levels can be derived from FIPS 199, which defines for all attributes the same three possible values: low, moderate, and high. In addition, the level has the option not to be applicable. Whichever scale is used, it is essential that organizations are able to select the level that applies to their needs.

As an example, for a single control, one could define the numeric confidentiality impact for low 0.1, medium 0.3, and high 1.0. All relevant security controls are associated with each scoring class or have a numerical impact value for all enumeration values. Scoring each control for each scoring class is not mandatory if the scoring class does not have an impact on the specific controls. For example, purely availability-protecting controls, such as the backup of data, are not scored for confidentiality. As a backup can be used to verify the integrity of data, the control can have lower numeric scoring for integrity.

The additions include an information security property (CIA) to provide controls based on organizational preferences. For example, an organization that handles a great deal of personal data can prioritize controls that protect confidentiality and integrity. Vice versa, a company having a limited amount of confidential data assets may prioritize the information availability and controls preserving it.

The score for each security control is calculated using the Weighted Sum Model (WSM) as the sum of the selected values for each control score attribute. WSM is a weighting method in MCDM [84]. Other weighting methods should also be considered based on the testing in the relevance cycle. When using WSM, denote the numeric score value associated with the j th option of the i th attribute

as $v_{i,j}$, and let s_i represent the index of the option selected by the user for the i th attribute. Then, the formula to calculate the control score would be as follows:

$$\text{Score} = \sum_{i=1}^n v_{i,s_i}$$

where:

- n is the total number of attributes,
- $v_{i,j}$ is the numeric value associated with the j th option of the i th attribute, and
- s_i is the index of the option selected by the user for the i th attribute.

Each control will eventually have a score that emphasizes the organization's priorities defined using preconditions. The controls with the highest scores are those that an organization should prioritize in the order of implementation of the controls. As a result, the scoring model will create a proposal for the organization's roadmap to enhance information security. Compared to the resource requirements of the traditional risk management approach to review all controls in a control catalog to find the relevant ones, the scoring model provides a roadmap with which to begin development.

The scoring model can be further developed in several ways. The new preconditions scored relevant to user organizations can be added to the model. However, this always requires analyzing the impact of new precondition attributes on the scoring results. Furthermore, the formula for calculating is very simple. It could be enhanced with statistical models to normalize the impact of different values. Especially, if the same controls are included in multiple use cases with high score values, the controls may obtain a score value where use case scores are overemphasized compared to other attribute values. Furthermore, the scoring model does not take into account the values of different asset types for organizations. This would require a model for asset valuation that would be suitable for organizations of all sizes and different financial appetites for risk realization. For information assets, asset-type scores can also be inherited from organizational information classification and labeling [4]. However, this requires either an organization-specific scoring model or a common information classification scheme such as national confidentiality levels.

5.4 Summary of artifacts

DSR aims to generate knowledge about how artifacts can and should be constructed or designed to achieve a desired set of goals [9]. During the research multiple iterations of rigor, relevance, and design cycles were executed.

The major development iterations of the SMW based artifact were presented in Articles III-V. Within each major development iteration, multiple rigor, relevance, and design cycles were performed to introduce new functionalities. A good example of the relationship of rigor and relevance cycles was the introduction of a risk taxonomy to classify identified risks in Article IV. In the relevance cycle, the need to group the risks in a hierarchy was identified. In rigor cycle, potential different risk taxonomies were analyzed and tested in wiki platform. Before the final solution was ready, both the rigor and relevance cycles were visited multiple times, and the design cycle was run continuously. Similarly, in Julkri development, precondition options for integrity and availability required various rigor cycle executions to identify the possible scales to measure required integrity and availability levels.

Articles III-V present the SMW-based platform, which organizations can use to select appropriate controls and collect information security risk details. The development started from the transformation of NIST SP 800-53 controls to SMW platform, but after several DSR cycles platform supported security control selection and risk management activities. Even the demonstrator produced was the concrete artifact created in the research, the research knowledge generated during the development was more significant artifacts. Where the demonstrator was used by a limited number of users, the research knowledge contributed to the development of Julkri, which has a more significant impact on society, which highlights the importance of the knowledge generated in DSR research.

The included articles represent the knowledge in a number of design artifacts as the result of research iterations. Some of the design artifacts are generalized and developed further as presented above. Table 6 summarizes the most important artifacts presented in the included articles and the derived artifacts. The derived artifacts are marked as "DA." To emphasize the different types of contributions to design knowledge, artifacts are categorized based on design theorizing modes according to the knowledge contributions that make Ω and λ .

The contribution of Ω -knowledge (comprising descriptive and explanatory knowledge [24]) includes comparisons of commonly used specifications, as well as statistical metadata. This knowledge was mostly created at the beginning of the research as part of the Articles I and II.

Contributions to λ -knowledge (prescriptive [24]) are divided into solution design entities and solution design knowledge. The solution design entities contributed by the research include the SMW-based control catalog instance and other artifacts required to import the data and add new functionality. These instances were developed in relevance cycles to evaluate different approaches to support the selection of the security control.

The contributed solution design knowledge consists of more abstract artifacts derived from solution design entities and the research process. These include the evaluation principles used and knowledge about their applicability. Julkri plays a specific role in research results. Although it is not a direct artifact of the research, the knowledge created by solution design in Articles III and IV was utilized in the development of the Julkri. In addition, improvements proposed to the security

TABLE 6 Summary of the artifacts created in the research

Knowledge type	Contributed artifacts
Ω : Knowledge about phenomena	<ul style="list-style-type: none"> • Comparison of ISO/IEC 27001:2013 and Katakri risk management requirements and their gaps (Article I) • Comparison of ISO/IEC 27002:2013 and Katakri security controls and their gaps (Article II) • Statistics of control relationships of NIST SP 800-53 controls (Article III)
λ : Solution design entities	<ul style="list-style-type: none"> • SMW-based security control catalog including semantic page templates (Article III) • Transformations of NIST SP 800-53 in OSCAL format to the SMW wiki object model (Articles III, IV) • Integration of a risk ontology into the control catalog object model (Article III) • Addition of security attributes to the control catalog (Article IV) • SMW page templates for risk management functionality (Article IV)
λ : Solution design knowledge	<ul style="list-style-type: none"> • Meta-model for an enhanced control catalog for SMW (Article IV, DA) • Communication SMW artifact research process and results (Articles III, IV, V) • Evaluation of SMW artifacts according to DSR principles and KIBP challenges (Article V) • Assessment of Julkri criteria as a DSR artifact (Article VI) • Enhancements to security audit criteria design guidelines (Article VI) • Process to utilize the enhanced control catalog (DA) • Control scoring model (DA)

audit criteria design principles are included in the contribution of solution design knowledge. The derived artifacts included further abstractions and aggregation of the knowledge gained from the development of the SMW artifacts and the Julkri development and evaluation process.

6 CONCLUSION

This chapter represents the results of the research, the limitations of the research, and the potential future work. Furthermore, the epilogue analyzes current potential of AI to support the security control selection.

6.1 Results

In this dissertation, the topic of security control selection as part of information and cyber-security risk management was approached using design science research methodology. Specifically, the idea was to evaluate and enhance security control catalogs to support SMEs in their selection of critical security controls for their operational environment. The first question to ask is: What did we have before?

When this research was started more than a decade ago, the security control catalogs contained lists of security controls suitable for organizations at that time. Organizations were expected to browse through all controls to select the most suitable to mitigate their threats as part of the risk management process. Security control catalogs have since been updated to respond to the current threat landscape. However, in a decade only limited enhancements have been made to support optimal security control selection. Recent versions of control catalogs have provided methods for filtering controls to reduce the competence and resource requirements of information and cyber-security risk management.

This dissertation includes six articles; the first two, Articles I and II, compared information security risk management processes and security control catalogs. Existing information security risk management methods and control catalogs have similarities, but also minor deviations. Based on the results of Articles I and II, hypotheses were made that security control selection can be enhanced to overcome competency and resource requirements.

Article III introduced the initial design iteration of an SMW platform-based security control catalog with advanced features. This design iteration provided an initial response to RQ1 by introducing new filtering and search functions

to the control catalog. At the time, the only publicly available control filtering solution was the NIST SP 800-53 supplementary website, where the user could filter out security controls based on the selected security baseline. The created artifact provided the basis for executing DSR rigor and relevance cycles to develop artifacts further in Article IV.

The improved version of the SMW-based artifact was developed further, and the results were presented in Article IV. In the enhanced version, information security risk management functions and an enhanced object model was introduced to support risk management activities. In particular, security controls were linked to the operational cyber-security risk taxonomy defined by Cebula et al. [10] to support the finding of security controls to mitigate specific risk categories. Additionally, to support control selection, CIA attributes were added to all controls. It should be noted that the enhanced version was developed before ISO/IEC 27002:2022, which includes a similar approach, was under development. The enhanced control catalog also included risk management features. Semantic forms were specified to add, modify, and retire risks, which allowed the user organization to manage risks within the wiki instance. While combining all features of the enhanced security control catalog, it allowed the user organization to find potential security controls based on risk taxonomy and information security attribute-based prioritization as well as maintain an organizational risk knowledge base. The artifact provides a partial answer to RQ1 that security control attributes support control selection, which was later confirmed with the development of the control catalogs, similar to the latest version of ISO/IEC 27002.

Article V focused on evaluating the development of the artifact presented in Articles II and IV from the DSR point of view. At the time of publication of the article, there was a very limited number of publications related to information and cyber security that applied the DSR methodology. As a result of the assessment, it was determined that the artifacts developed met the common requirements of DSR work that provide solutions to wicked problems. In general, the research process implemented has been design and development centered to follow the steps of the DSR of Peffers et al. [70], where the steps executed included design and development (Articles I-IV and VI), demonstration (Articles II-V), evaluation (Articles V-VI), and communication (all articles and this dissertation).

The second question to ask is the following: What we have now? Article VI answers this question and concludes this research by combining RQ1 and RQ2. First, the development of Julkri adapted many results published in Articles III and IV, providing novel approaches to select and prioritize security controls from the control catalog using preconditions defined by the user. This approach requires the user to be able to provide basic information on organizational information and cyber-security priorities and asset types, but as a result, it reduces resource requirements to assess potential security controls. Especially Julkri use cases or similar NIST RMF overlays provide an efficient mechanism to select subsets of security controls from exhaustive control catalogs. It would also be applicable to use even attributes in combination with use-case definitions, as Julkri does, to prioritize controls even more in specific scenarios. Second, Article VI analyzes

Julkri as a DSR artifact. As a result of the evaluation, Julkri makes significant improvements as a security control catalog compared to its predecessor and other commonly used security control catalogs. However, it points out that the DSR methodology could be expanded to support domain- and artifact-specific evaluation criteria to the information security domain.

The first research question (RQ1) was to analyze how security control catalogs can be enhanced to support SME organizations' information and cyber security, especially in security control selection, without a complex risk assessment process. As a conclusion in Articles III, IV, and VI, from a security control implementer point of view, it is easier for non-security-oriented organizations to identify security goals and use cases as preconditions for a control set than reviewing lists of hundreds of security controls, trying to identify the relevant ones. Where the common approach has previously been that the organization should familiarize itself with all controls and then select the appropriate ones, the recent development of ISO/IEC 27002, which advises the filtering of exhaustive security control catalogs, is required to be developed further. As the results show, there are a number of attributes that can be used to prioritize security control selection and to focus on relevant security controls. The scoring model presented as a derived artifact will work similar to a security consultant asking organizational properties, goals, and priorities and then providing suggestions based on the preconditions and expert knowledge embedded in the knowledge base. As Article VI highlights, attributes were used in the Julkri criteria to apply the knowledge of information security experts to prioritize security controls without a complex quantitative risk management approach.

The second research question (RQ2) asked under what conditions can the DSR methodology be utilized in the development of information security artifacts. As the response to the research question RQ2, DSRM is a suitable research method for conducting design-oriented information and cyber-security research; however, there is a research gap for information security domain-specific evaluation frameworks. As DSR has been used modestly in cyber and information security research compared to information systems (IS) research, a research gap was identified to determine how DSR could be used better in information and cyber-security research. As DSR originates from IS research, there are IS-related DSR theories and evaluation methods, which the information and cyber-security research domains lack. As has been shown, DSR is a suitable method to create practical solutions to wicked information and cyber-security problems, though there is still more to develop from the methodology point of view.

The outcome of this dissertation is a set of artifacts and design knowledge supporting the selection of information and cyber-security controls. SMW knowledge base versions provided features at the time of publication that were not available in common security control catalogs. Although Julkri is not an imminent artifact of the research, multiple results and ideas from preceding artifacts were utilized in the development of Julkri. Another artifact is the process and learning from it, as often in DSR work. Research shows that there is a place for design-oriented information and cyber-security research to produce new artifacts

for practical use cases.

6.2 Limitations

There is one limitation of the research that is common to many other DSR projects; the long-lasting testing of the artifacts. All of the developed artifacts could have been tested more in real use by performing more relevance and design cycles. As noted in Article VI, the Julkri criteria were also not comprehensively tested during development and, therefore, lacked the real-world testing of all potential use cases during the time of publication. The same applies to artifacts developed in Articles III and IV, which have not been extensively tested in real-world scenarios; only common risk management process use cases were employed in the testing. Although functionality is based on common risk management activities, and hence, basic verification is performed, it is possible that some deficiencies could be detected in extensive real-world verification.

The limitations of DSR research evaluation include the development of new evaluation criteria for information security assets. Although the evaluation criteria of Kelo et al. [56] used in Article VI were found to be not sufficient for assets, the article did not present an updated version of the design principles and evaluation criteria. This is a topic for further research.

6.3 Future work

In design science, the research process will never be completed. There is always something to develop, either from the application domain or in the scientific foundation. Hence, the last question to ask is: What will happen in the future?

As there have been some recent developments from the standards perspective, such as the OSCAL format and the new version of ISO/IEC 27002:2022, there is much potential advancement in research and tool development in the future. Further research is required to evaluate how practitioners utilize the new attributes of ISO/IEC 27002 and Julkri. Where Julkri forces the use of preconditions, it would also be essential to evaluate how consistently preconditions are set for different assessment targets.

Another future practical study area is the analysis of CIA properties, which would provide a basis for consistent risk assessment results. Confidentiality levels have been defined in various approaches, including generic-level definitions in FIPS 199 [87]. In addition, availability definitions have been based on acceptable system downtime. However, integrity is an information security property that does not have such scales available. During Julkri development, a limited number of scales were found, but they were not as descriptive as confidentiality and availability metrics. Therefore, they were suspected to result in inconsistent

assessment results.

It was also identified that to reuse security control catalogs, it is important that specifications are available in a structured, machine-readable format such as OSCAL. Publicly available and structured information allows the development of new solutions to manage information security risks and compliance. Where ISO/IEC 27002 is one of the rare widely used security catalogs that is not freely available, NIST SP 800-53 is the opposite, being freely available in multiple machine-readable formats. As OSCAL is a newly introduced approach, there are not yet many tools to support it. The future will show how it will be used and will provide a common format for compliance assessment tools and criteria.

During the development of Julkri, the topic of psychological issues of information security risk management, especially control selection, was raised, especially if the regulatory pressure of government authorities forces the implementation of security controls that lack a reasonable cost-benefit ratio. Psychological issues of risk management have been researched [63], but not human factors related to the selection of security controls. An interesting aspect would be to research excessive control selection, which conflicts with the common risk management objective to implement controls with a positive ROI.

During the research, it was identified that all control catalogs have overlapping definitions with only minor differences. Additionally, recent versions of control catalogs contain cross-references to others to help verify that the contents are similar. However, there has been very little criticism about which security controls actually provide the most cost-effective protection. As the contents of new catalogs are almost always based on previous versions and other catalogs, a critical objective analysis of each control should be performed to avoid keeping controls with a low cost-benefit ratio in the common catalogs.

Finally, the scoring model presented in Section 5.3 provides the next design iteration of the control selection logic utilized in Julkri. It combines characteristics of multi-criteria decision making to provide practical solution for information security risk management. Although this design iteration is still under development, it also highlights the nature of the continuous development of DSRM.

In conclusion, during the research, security control catalogs modestly developed to support the selection of security controls during the last decade. However, as presented, there are still practical opportunities to develop new approaches to support the selection of security controls and help organizations improve information and cyber security and business continuity. DSR provides a design methodology to further develop these opportunities to create practical solutions for all organizations. Although information security is still considered an essential problem for SME organizations, there is still a need for the new evolution of solutions.

6.4 Epilogue

AI represents a technological leap that transcends traditional computing paradigms, offering unprecedented capabilities in problem solving using natural language [11, 88]. It will and already has changed information and cyber security on both sides, as new threats emerge and as mitigation methods to respond to existing and emerging threats. It will also provide new means for security control selection and decision support. Chat-based interfaces provide a security consultant-like experience, which can be used to analyze organizational security postures and select potential security controls. In AI and machine learning, a flawless and accurate training data set is essential for consistent and valid results [42]. To analyze the current performance of AI platforms, an additional test was performed using ChatGPT 3.5 by OpenAI and Copilot by Microsoft. The test aimed to analyze the prioritization capabilities of the security controls of AI platforms. Details of the test setup and the results are presented in Appendix 1.

As the results show, there are significant differences in the responses of these two AI platforms to the eight questions presented. Where ChatGPT's answers to questions include 38 different security controls, Copilot's answers include only 16 different controls. ChatGPT's responses change significantly when the questions highlight different priorities for the user, whereas Copilot's changes are very limited and focus mainly on changing the priority order of the same control set. In ChatGPT's responses, there is a significant difference based on which information security property, confidentiality, integrity, or availability, is prioritized. Copilot is more transparent and shows the training data for each control as a reference, whereas ChatGPT does not provide references. Microsoft Copilot's references for the controls provided are from only two sources: mainly from the SME Guide on Information Security Controls [86] and the Cybersecurity Guide for SMEs [20] by ENISA. Due to transparency, it is easy to assess that Copilot's results are very limited, although both primary sources are still relevant on a general level to all SMEs. Amending the question of minimal resources indicates that the actual implementation costs of the security controls are not covered in the learning data, as the results of the questions include multiple controls that are not feasible for organizations with minimal resources. One reason for this is that the actual implementation costs of even widely used security controls are not available.

In summary, the results of this dissertation can also be used to develop AI language models further and find deficiencies in learning data. It can also improve the quality of decision making as learning data can include information that is currently too resource consuming to analyze during risk assessment. At the moment of this writing, AI can provide a starting point for information development for an SME, but requires careful validation of the provided guidance. Especially in the chat user interface, the response quality depends on the prompting capabilities of the user. When language models and learning data are further enhanced, AI-based solutions can provide a cost-effective security consultant to support SMEs in the development of information security.

YHTEENVETO (SUMMARY IN FINNISH)

Tietoturvallisuuden hallintakeinojen valinta

Nykyaikaisessa toimintaympäristössä kaikkien organisaatioiden on huomioitava tieto- ja kyberturvallisuus toiminnan jatkuvuuden varmistamiseksi. Tieto- ja kyberturvallisuuden riskienhallintaan on olemassa useita menetelmiä, mutta ne soveltuvat kuitenkin yleisesti ottaen huonosti pienille ja keskisuurille yrityksille edellyttämiensä resurssien vuoksi. Tehokkaassa tieto- ja kyberturvallisuuden hallinnassa korostuu organisaation kannalta oikeiden hallintakeinojen valinta, jolloin käytävissä olevat resurssit kohdistuvat tehokkaimmin organisaation kriittisten kohteiden suojaamiseen. Hallintakeinot ovat niitä hallinnollisia, teknisiä ja fyysisen turvallisuuden menetelmiä, joilla organisaatio varmistaa tietoturvallisuuden eli tiedon luottamuksellisuuden, eheyden ja saatavuuden.

Väitöskirjan tavoitteena on vastata seuraaviin tutkimuskysymyksiin:

RQ1 Kuinka tietoturvallisuuden hallintakeinojen luetteloita voidaan kehittää tukemaan PK-yritysten tieto- ja kyberturvallisuuden hallintakeinojen valintaa ilman monimutkaisia riskienarviointiprosesseja?

RQ2 Millä edellytyksillä suunnittelutiedettä voidaan hyödyntää tieto- ja kyberturvallisuuden artefaktien kehittämisessä?

Tutkimuksen kahdessa ensimmäisessä artikkelissa I ja II arvioitiin tietoturvariskienhallinnan menetelmiä ja hallintakeinojen luetteloita. Näiden perusteella kehitettiin Semantic MediaWikiin perustuva artefakti tietoturvallisuuden hallintakeinojen valintaan, jota on esitelty artikkeleissa III ja IV. Tutkimuksessa aineistona käytettiin NIST SP 800-53 hallintakeinojen luettelo, joka on vapaasti saatavissa rakenteellisessa koneluettavassa muodossa. Se on yksi laajimmista yleisesti käytetyistä hallintakeinojen luetteloista sisältäen yli tuhat tietoturvallisuuden hallintakeinoa ja hallintakeinon laajennusta. Hallintakeinot tuotiin wiki-järjestelmään, jossa tietomallia laajennettiin erilaisilla määritteillä hallintakeinojen valinnan helpottamiseksi. On huomattava, että tutkimus on tapahtunut ajallisesti pitkällä, yli kymmenen vuoden, aikavälillä ja tutkimuksen ensimmäisten artikkeleiden julkaisuaikana tunnetuimmat hallintakeinojen luettelot, kuten ISO/IEC 27002, NIST SP 800-53 ja CIS Controls, eivät tukeneet hallintakeinojen valintaa kuin enintään yksinkertaisella priorisoinnilla. Uusimmissa versioissa luetteloissa on kuitenkin huomioitu jo vastaavia määritteitä kuin näitä ennen tuotetussa artefaktissa.

Tutkimuksessa käytettiin suunnittelutiedettä menetelmänä arvioimaan tuotettuja artefakteja. Artikkelissa V arvioitiin aiemmissa artikkeleissa esiteltyä tietoturvallisuuden hallintakeinojen luettelo. Suunnittelutiedettä on käytetty yleisesti tietojärjestelmien kehittämiseen liittyvässä tutkimuksessa, mutta tietoturvallisuuden menetelmien kehittämisen tutkimuksessa sitä ei ole juurikaan käytetty. Osana tutkimusta arvioitiin suunnittelutiedettä menetelmänä tietoturvallisuuden artefaktien kehittämisessä. Tutkimuksen ensimmäisessä artefaktissa kehitettyjä ominaisuuksia käytettiin hyväksi Julkri-kriteeristön kehityksessä, jota arvioitiin

suunnittelutieteen kriteerein osana tutkimusta artikkelissa VI. Julkri on kehitetty arvioimaan tiedonhallintayksiköiden ja niiden palveluntuottajien tietoturvallisuuden tasoa julkisen hallinnon tiedonhallinnasta annetun lain mukaisesti. Kehitystyössä pyrittiin kehittämään arviointikriteeristö, joka soveltuu kaikenkokoisille tiedonhallintayksiköille alkaen pienimmistä kunnista ja niiden palveluntuottajista aina suurimpiin julkishallinnon yksiköihin.

Ensimmäisen tutkimuskysymyksen RQ1 osalta Julkri-kriteeristöissä toteutettu laadulliseen riskienhallintaan perustuva malli perustuu aiempia menetelmiä enemmän riskilähtöiseen hallintakeinojen valintaan, jolloin olennaisia toteutettavia hallintakeinoja on vähemmän. Olennaisten hallintakeinojen lisäksi käyttäjälle annetaan riskitasoon perustuvia ehdotuksia mahdollisista hallintakeinoista arvioitavaksi. Siten esiehtojen perusteella laajasta hallintakeinojen luettelosta voidaan osoittaa pienempi, asiantuntijatietoon perustuva osajoukko organisaation itsensä arvioitavaksi toteutusta varten. Tutkimuksen tuloksena voidaan osoittaa, että erilaisiin esiehtoihin ja käyttötapauksiin perustuvilla ennakkotiedoilla voidaan helpottaa hallintakeinojen valintaa ja vähentää hallintakeinojen luettelon käyttäjältä edellytettävää tietoturvaosaamista. Priorisoinnin perusteella organisaatiot voivat kohdistaa käytettävissä olevat resurssit todennäköisemmin parhaimman hyötysuhteen antaviin hallintakeinoihin.

Toisen tutkimuskysymyksen RQ2 osalta tulokset osoittavat, että suunnittelutiedettä voidaan käyttää myös muiden tietoturvallisuuden artefaktien kuin tietojärjestelmien kehityksessä. Artefaktien arviointia varten kuitenkin tulisi kehittää edelleen arviointikriteerejä, jotka soveltuvat erityisesti tieto- ja kyberturvallisuuden artefaktien arviointiin suunnittelutieteen yleisiä arviointikriteerejä paremmin.

Tutkimuksen osalta tunnistettiin myös mahdollisuus hyödyntää tutkimuksen lopputuloksia lähitulevaisuudessa tekoälyn kielimallien kehittämisessä. Käytämällä hyväksi tunnistettuja ominaispiirteitä osana kielimalleja, voidaan tekoälyalustat saada tuottamaan kysyjän tilanteeseen paremmin sopivia vastauksia. Näiltä osin tulee kuitenkin huomioida, että on ehdottoman tärkeää varmistua opetuksessa käytettävän aineiston eheydestä, jotta tekoälyalustojen tuottamat vastaukset ovat oikeita kyseisessä tilanteessa. Opetusaineiston tulee siis perustua asiantuntijatietoon eikä vain vapaasti saatavilla olevaan yleiseen tietoon, jotta hallintakeinojen valinta perustuu muihinkin näkökulmiin kuin aiempien hallintakeinojen luetteloiden sisältöön.

BIBLIOGRAPHY

- [1] *Act on Information Management in Public Administration (906/2019)*. Ministry of Finance. 2019. URL: <https://www.finlex.fi/en/laki/kaannokset/2019/en20190906.pdf>.
- [2] Abdulmajeed Alahmari and Bob Duncan. "Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence". In: *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*. IEEE. 2020, pp. 1–5.
- [3] Arina Alexei (Lachi). "Implementing Design Science Research Method to Develop a Cyber Security Framework for HEIs in Moldova". In: *Electronics, Communications and Computing IC|ECCO-2021*. Chişinău: Technical University of Moldova, 2021, pp. 228–231. DOI: 10.52326/ic-ecco.2021/NWC.02.
- [4] Christianah Yetunde Alonge, Oluwasefunmi Tale Arogundade, Kayode Adesemowo, Friday Thomas Ibrahalu, Olusola John Adeniran, and Abiodun Muyideen Mustapha. "Information Asset Classification and Labelling Model Using Fuzzy Approach for Effective Security Risk Assessment". In: *2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS)*. 2020, pp. 1–7. DOI: 10.1109/ICMCECS47690.2020.240911.
- [5] Øystein Amundrud, Terje Aven, and Roger Flage. "How the definition of security risk can be made compatible with safety definitions". In: *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 231.3 (2017), pp. 286–294.
- [6] *Assessment criteria for information security in public administration (Julkri)*. Publications of the Ministry of Finance 2022:74. 2022. URL: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164440/VM_2022_74.pdf.
- [7] Terje Aven. "Risk assessment and risk management: Review of recent advances on their foundation". In: *European Journal of Operational Research* 253.1 (2016), pp. 1–13.
- [8] Frode Mathias Bekkevik, Ole Reidar Holm, Polyxeni Vassilakopoulou, and Eli Hustad. "Information security practices in organizations: A literature review on challenges and related measures". In: *Digital and social transformation for a better society-Proceedings of the Twelfth Mediterranean Conference on Information Systems (MCIS 2018)*. 2018.
- [9] Jan vom Brocke, Alan Hevner, and Alexander Maedche. "Introduction to Design Science Research". In: *Design Science Research. Cases*. Ed. by Jan vom Brocke, Alan Hevner, and Alexander Maedche. Springer International Publishing, 2020, pp. 1–13.
- [10] James J Cebula, Mary E Popeck, and Lisa R Young. "A taxonomy of operational cyber security risks version 2". In: *Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, Tech. Rep. CMU/SEI-2014-TN-006* (2014).

- [11] Souradip Chakraborty, Amrit Singh Bedi, Sicheng Zhu, Bang An, Dinesh Manocha, and Furong Huang. *On the possibilities of AI-generated text detection*. arXiv:2304.04736. 2023.
- [12] Sunil Chaudhary, Vasileios Gkioulos, and Sokratis Katsikas. "A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises". In: *Computer Science Review* 50 (2023), p. 100592. URL: <https://www.sciencedirect.com/science/article/pii/S157401372300059X>.
- [13] Alladean Chidukwani, Sebastian Zander, and Polychronis Koutsakis. "A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations". In: *IEEE Access* 10 (2022), pp. 85701–85719.
- [14] *CIS Critical Security Controls V8*. Center for Internet Security. 2021. URL: <https://www.cisecurity.org/controls>.
- [15] Michael Coole, Jeff Corkill, and Andrew Woodward. "Defence in depth, protection in depth and security in depth: A comparative analysis towards a common usage language". In: SRI Security Research Institute, Edith Cowan University, Perth, Western Australia, 2012.
- [16] Anthony Cox Jr. "What's wrong with risk matrices?" In: *Risk Analysis* 28.2 (2008), pp. 497–512.
- [17] *Cyber Security and Australian Small Businesses: Results from the Australian Cyber Security Centre Small Business Survey*. Australian Cyber Security Centre. 2023. URL: <https://www.cyber.gov.au/sites/default/files/2023-03/Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results%20-%2020201130.pdf>.
- [18] *Cyber security breaches survey 2023*. UK Government, Department for Science, Innovation & Technology. 2023. URL: <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023>.
- [19] *Cybersecurity Capability Maturity Model (C2M2) v2.1*. U.S. Department of Energy. 2022. URL: <https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf>.
- [20] *Cybersecurity guide for SMEs – 12 steps to securing your business*. European Union Agency for Cybersecurity. 2021. URL: <https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes>.
- [21] John DeLong. "Aligning the Compasses: A Journey through Compliance and Technology". In: *IEEE Security & Privacy* 12.4 (2014), pp. 85–89. DOI: 10.1109/MSP.2014.62.
- [22] Antonio Dennis, Rohana Jones, Duane Kildare, and Corlane Barclay. "Design science approach to developing and evaluating a national cybersecurity framework for Jamaica". In: *The Electronic Journal of Information Systems in Developing Countries* 62.1 (2014), pp. 1–18.

- [23] *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. European Union. 2022. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02022L2555-20221227&qid=1712930003806>.
- [24] Andreas Drechsler and Alan R Hevner. "Utilizing, producing, and contributing design knowledge in DSR projects". In: *Designing for a Digital and Globalized World: 13th International Conference, DESRIST 2018, Chennai, India, June 3–6, 2018, Proceedings 13*. Springer. 2018, pp. 82–97.
- [25] Shannon Eggers and Katya Le Blanc. "Survey of cyber risk analysis techniques for use in the nuclear industry". In: *Progress in Nuclear Energy* 140 (2021), p. 103908.
- [26] Kaan Eyilmez, Ali Basyurt, Stefan Stieglitz, Christoph Fuchss, Marc-André Kaufhold, Christian Reuter, and Milad Mirbabaie. "A Design Science Artefact for Cyber Threat Detection and Actor Specific Communication". In: *ACIS 2022 Proceedings*. 2022, p. 50. URL: <https://aisel.aisnet.org/acis2022/50>.
- [27] Stefan Fenz and Andreas Ekelhart. "Verification, Validation, and Evaluation in Information Security Risk Management". In: *IEEE Security and Privacy* 9.2 (2011), pp. 58–65. DOI: 10.1109/MSP.2010.117.
- [28] Stefan Fenz, Andreas Ekelhart, and Thomas Neubauer. "Information security risk management: In which security solutions is it worth investing?". In: *Communications of the Association for Information Systems* 28.1 (2011), p. 22.
- [29] Stefan Fenz, Johannes Heurix, Thomas Neubauer, and Fabian Pechstein. "Current challenges in information security risk management". In: *Information Management & Computer Security* 22.5 (2014), pp. 410–430.
- [30] *Framework for Improving Critical Infrastructure Cybersecurity v1.1*. National Institute of Standards and Technology. 2018. URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
- [31] Joshua M. Franklin, ed. *Implementation Guide for Small- and Medium-Sized Enterprises: CIS Controls Implementation Group 1, Version 2.0*. Center for Internet Security, 2023. URL: https://learn.cisecurity.org/CIS-Controls-Implementation-Guide-for_SMEs.
- [32] Lawrence A. Gordon and Martin P. Loeb. "The Economics of Information Security Investment". In: *ACM Trans. Inf. Syst. Secur.* 5.4 (Nov. 2002), pp. 438–457. DOI: 10.1145/581271.581274.
- [33] S. G. Govender, M. Loock, E. Kritzinger, and S. Singh. "Using Design Science Research to Iteratively Enhance Information Security Research Artefacts". In: *Networks and Systems in Cybernetics*. Ed. by Radek Silhavy and Petr Silhavy. Springer International Publishing, 2023, pp. 49–61. ISBN: 978-3-031-35317-8.

- [34] *Government Decree on Security Classification of Documents in Central Government (1101/2019)*. Ministry of Finance. 2019. URL: <https://www.finlex.fi/en/laki/kaannokset/2019/en20191101.pdf>.
- [35] Shirley Gregor and Alan R Hevner. "Positioning and presenting design science research for maximum impact". In: *MIS quarterly* (2013), pp. 337–355.
- [36] Stjepan Groš. "A Critical View on CIS Controls". In: *2021 16th International Conference on Telecommunications (ConTEL)*. 2021, pp. 122–128. DOI: 10.23919/ConTEL52528.2021.9495982.
- [37] Margareta Heidt, Jin P Gerlach, and Peter Buxmann. "Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments". In: *Information Systems Frontiers* 21 (2019), pp. 1285–1305.
- [38] Peter Heinrich, Axel Uhl, and Monika Josi. "Designing for knowledge based cyber-security: episode 1: what should we teach?" In: *26th European Conference on Information Systems (ECIS 2018), Portsmouth, UK, 23-28 June 2018*. Association for Information Systems. 2018.
- [39] Alan Hevner. "A Three Cycle View of Design Science Research". In: *Scandinavian Journal of Information Systems* 19 (Jan. 2007).
- [40] Alan Hevner and Samir Chatterjee. *Design Research in Information Systems: Theory and Practice*. Vol. 22. Integrated Series in Information Systems. Springer, 2010. ISBN: 9781441956521.
- [41] Alan R. Hevner, Salvatore T. March, Jinsoo Park, and Sudha Ram. "Design Science in Information Systems Research". In: *MIS Quarterly* 28.1 (2004), pp. 75–105. URL: <http://www.jstor.org/stable/25148625>.
- [42] Amani Ibrahim, Dhananjay Thiruvady, Jean-Guy Schneider, and Mohamed Abdelrazek. "The challenges of leveraging threat intelligence to stop data breaches". In: *Frontiers in Computer Science* 2 (2020), p. 36.
- [43] Juhani Iivari. "A paradigmatic analysis of information systems as a design science". In: *Scandinavian Journal of Information Systems* 19.2 (2007), pp. 39–64.
- [44] Öyku Isik, Joachim Van den Bergh, and Willem Mertens. "Knowledge intensive business processes: an exploratory study". In: *2012 45th Hawaii International Conference on System Sciences*. IEEE. 2012, pp. 3817–3826.
- [45] Olfa Ismail. "Designing information security culture artifacts to improve security behavior: An evaluation in SMEs". In: *International Conference on Design Science Research in Information Systems and Technology*. Springer. 2022, pp. 319–332.
- [46] *ISO 55000:2014. Asset management – Overview, principles and terminology*. International Organization for Standardization. Geneva, 2014. URL: <https://www.iso.org/standard/55088.html>.

- [47] ISO/IEC 27005:2022. *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*. 4th. International Organization for Standardization. Geneva, 2022. URL: <https://www.iso.org/standard/80585.html>.
- [48] ISO/IEC 15408-1:2022. *Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model*. 4th. International Organization for Standardization. Geneva, 2022. URL: <https://www.iso.org/standard/72891.html>.
- [49] ISO/IEC 27000:2018. *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. 5th. International Organization for Standardization. Geneva, 2018. URL: <https://www.iso.org/standard/73906.html>.
- [50] ISO/IEC 27001:2022. *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*. 3rd. International Organization for Standardization. Geneva, 2022. URL: <https://www.iso.org/standard/27001>.
- [51] ISO/IEC 27002:2022. *Information security, cybersecurity and privacy protection – Information security controls*. 3rd. International Organization for Standardization. Geneva, 2022. URL: <https://www.iso.org/standard/75652.html>.
- [52] *IT-Grundschutz-Compendium*. Federal Office for Information Security (BSI), Bonn. 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf.
- [53] Leighton Johnson. *Security controls evaluation, testing, and assessment handbook*. Academic Press, 2019.
- [54] Mouna Jouini, Latifa Ben Arfa Rabai, and Anis Ben Aissa. “Classification of Security Threats in Information Systems”. In: *Procedia Computer Science* 32 (2014), pp. 489–496. DOI: 0.1016/j.procs.2014.05.452. The 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), the 4th International Conference on Sustainable Energy Information Technology (SEIT-2014).
- [55] *Katakri 2020: Information Security Audit Tool for Authorities*. National Security Authority of Finland. 2021. URL: https://um.fi/documents/35732/0/FINAL++Katakri-2020_201218_en.pdf.
- [56] Tomi Kelo, Juhani Eronen, and Kimmo Rousku. “Enhanced Model for Efficient Development of Security-Audit Criteria”. In: *Journal of Information Warfare* 17.3 (2018), pp. 50–63.
- [57] Barbara Krumay, Edward W. N. Bernroider, and Roman Walser. “A Framework to Achieve Cybersecurity Accountability of Critical Infrastructure Providers: A Design Science Research Approach”. In: *Organizing in a Digitized World*. Ed. by Stefano Za, Augusta Consorti, and Francesco Virili. Cham: Springer International Publishing, 2022, pp. 233–248.

- [58] Yevhenii Kurii and Ivan Opirskyy. “Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013”. In: *Proceedings of the CEUR Workshop 3288* (2022), pp. 21–32.
- [59] *Kybermittari – Cybermeter v2.1*. National Security Authority of Finland. 2024. URL: <https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter>.
- [60] Romanescu Marcel Laurențiu. “Importance of SMEs in European countries economy”. In: *Annals of the „Constantin Brâncuși” University of Târgu Jiu, Economy Series 3* (2016), pp. 174–155.
- [61] Georgia Lykou, Argiro Anagnostopoulou, and Dimitris Gritzalis. “Implementing cyber-security measures in airports to improve cyber-resilience”. In: *2018 Global Internet of Things Summit (GIoTS)*. IEEE. 2018, pp. 1–6.
- [62] Davor Maček, Ivan Magdalenić, and Nina Begičević Redepd. “A systematic literature review on the application of multicriteria decision making methods for information security risk assessment”. In: *International Journal of Safety and Security Engineering* 10.2 (2020), pp. 161–174. DOI: 10.18280/ijssse.100202.
- [63] Ahmed A. Moustafa, Abubakar Bello, and Alana Maurushat. “The Role of User Behaviour in Improving Cyber Security Management”. In: *Frontiers in Psychology* 12 (2021). DOI: 10.3389/fpsyg.2021.561011.
- [64] Alva Hendi Muhammad, Joko Dwi Santoso, and Ananda Fikri Ijlal Akbar. “Information security investment prioritization using best-worst method for small and medium enterprises”. In: *Indonesian Journal of Electrical Engineering and Computer Science* 31.1 (2023), pp. 271–280.
- [65] Nicolas Mundbrod and Manfred Reichert. “Process-aware task management support for knowledge-intensive business processes: findings, challenges, requirements”. In: *2014 IEEE 18th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations*. IEEE. 2014, pp. 116–125.
- [66] *NIST Risk Management Framework: Control Overlay Repository*. National Institute of Standards and Technology. URL: <https://csrc.nist.gov/projects/risk-management/sp800-53-controls/overlay-repository>.
- [67] Marie Caroline Oetzel and Sarah Spiekermann. “A systematic methodology for privacy impact assessments: a design science approach”. In: *European Journal of Information Systems* 23.2 (2014), pp. 126–150.
- [68] *OSCAL: the Open Security Controls Assessment Language*. Last updated on November 8, 2023. URL: <https://pages.nist.gov/OSCAL/>.
- [69] Jyri Paasonen and Mikko Luomala. “Tietosuojaan viranomaisvalvonnan ja seuraamusjärjestelmän kehitys-tarkastelussa tietosuojavaltuutetun ja seuraamuskollegian päätöksiä vuosilta 2018–2022”. In: *Defensor Legis* 1 (2024), pp. 40–66. DOI: 10.2753/MIS0742-1222240302.

- [70] Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger, and Samir Chatterjee. "A Design Science Research Methodology for Information Systems Research". In: *Journal of Management Information Systems* 24.3 (2007), pp. 45–77. DOI: 10.2753/MIS0742-1222240302.
- [71] Shari Pfleeger and Robert Cunningham. "Why Measuring Security Is Hard". In: *IEEE Security and Privacy* 8.4 (2010), pp. 46–54. DOI: 10.1109/MSP.2010.60.
- [72] Jyri Rajamäki. "Challenges to a Smooth-Running Data Security Audits. Case: A Finnish National Security Auditing Criteria KATAKRI". In: *2014 IEEE Joint Intelligence and Security Informatics Conference*. 2014, pp. 240–243. DOI: 10.1109/JISIC.2014.45.
- [73] Jyri Rajamäki. "Design Science Research Towards Ethical and Privacy-Friendly Maritime Surveillance ICT Systems". In: *Digital Transformation, Cyber Security and Resilience of Modern Societies*. Ed. by Todor Tagarev, Krasimir T. Atanassov, Vyacheslav Kharchenko, and Janusz Kacprzyk. Springer International Publishing, 2021, pp. 95–115. DOI: 10.1007/978-3-030-65722-2_7.
- [74] Jyri Rajamäki and Rauno Pirinen. "Design science research towards resilient cyber-physical eHealth systems". In: *Finnish Journal of eHealth and eWelfare* 9.2-3 (May 2017), pp. 203–216. DOI: 10.23996/fjhw.61000. URL: <https://journal.fi/finjehew/article/view/61000>.
- [75] Nisha Rawindaran, Ambikesh Jayal, Edmond Prakash, and Chaminda Hewage. "Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales". In: *International Journal of Information Management Data Insights* 3.2 (2023). DOI: 10.1016/j.jjime.2023.100191.
- [76] AM Rea-Guaman, T San Feliu, JA Calvo-Manzano, and Isaac Daniel Sánchez-García. "Systematic review: cybersecurity risk taxonomy". In: *International Conference on Software Process Improvement*. Springer. 2017, pp. 137–146.
- [77] Tony Sager. *Cybersecurity at Scale: Piercing the Fog of More*. URL: <https://www.cisecurity.org/insights/blog/cyber-at-scale-piercing-the-fog-of-more> (visited on 04/30/2024).
- [78] Anna Sarri, Viktor Paggio, and Georgia Bafoutsou. *Cybersecurity for SMEs: Challenges and Recommendations*. European Union Agency for Cybersecurity (ENISA), Heraklion. 2021. URL: <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>.
- [79] Christopher Schmitz, Michael Schmid, David Harborth, and Sebastian Pape. "Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities". In: *Computers and Security* 108 (2021), p. 102306. DOI: 10.1016/j.cose.2021.102306.
- [80] *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53, Rev. 5. National Institute of Standards and Technology, 2020. URL: <https://doi.org/10.6028/NIST.SP.800-53r5>.

- [81] Alireza Shameli-Sendi, Rouzbeh Aghababaei-Barzegar, and Mohamed Cheriet. "Taxonomy of information security risk assessment (ISRA)". In: *Computers & security* 57 (2016), pp. 14–30.
- [82] Mario Silic and Paul Benjamin Lowry. "Using design-science based gamification to improve organizational security training and compliance". In: *Journal of management information systems* 37.1 (2020), pp. 129–161.
- [83] Tanita Singano, Hombakazi Ngejane, Crestinah Mudau, Lungisani Ndlovu, and Mkhululi Tyukala. "ML-Based Security Analytics in South African SMEs: A Review and Classification". In: *2023 International Conference on Electrical, Computer and Energy Technologies (ICECET)*. 2023, pp. 1–6. DOI: 10.1109/ICECET58911.2023.10389479.
- [84] Meenu Singh and Millie Pant. "A review of selected weighing methods in MCDM with a case study". In: *International Journal of System Assurance Engineering and Management* 12 (2021), pp. 126–144.
- [85] *SME Guide for the implementation of ISO IEC 27001 on Information Security Management*. Small Business Standards. URL: <https://sbs-sme.eu/wp-content/uploads/2024/02/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management-min-1-2.pdf>.
- [86] *SME Guide on Information Security Controls*. Small Business Standards. 2022. URL: https://sbs-sme.eu/wp-content/uploads/2024/01/SBS-SME-Guide_Information-Security-Controls.pdf.
- [87] *Standards for Security Categorization of Federal Information and Information Systems*. FIPS PUB 199. National Institute of Standards and Technology, 2004. URL: <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf>.
- [88] Stefan Strauß. "From big data to deep learning: a leap towards strong AI or 'intelligentia obscura'?" In: *Big Data and Cognitive Computing* 2.3 (2018), p. 16.
- [89] Edyta Karolina Szczepaniuk, Hubert Szczepaniuk, Tomasz Rokicki, and Bogdan Klepacki. "Information security assessment in public administration". In: *Computers and Security* 90 (2020), p. 101709. DOI: 10.1016/j.cose.2019.101709.
- [90] Hamedand Tabrizchi and Marjan Kuchaki Rafsanjani. "A survey on security challenges in cloud computing: issues, threats, and solutions". In: *The Journal of Supercomputing* 76.12 (Dec. 2020), pp. 9493–9532. DOI: 10.1007/s11227-020-03213-1.
- [91] John Venable. "Design Science Research Post Hevner et al.: Criteria, Standards, Guidelines, and Expectations". In: *Global Perspectives on Design Science Research*. Ed. by Robert Winter, J. Leon Zhao, and Stephan Aier. Berlin: Springer, 2010, pp. 109–123. ISBN: 978-3-642-13335-0.
- [92] John Venable and Richard Baskerville. "Eating our own cooking: Toward a more rigorous design science of research methods". In: *Electronic Journal of Business Research Methods* 10.2 (2012), pp. 141–153.

- [93] John Venable, Jan Pries-Heje, and Richard Baskerville. "FEDS: a framework for evaluation in design science research". In: *European Journal of Information Systems* 25 (2016), pp. 77–89.
- [94] Jiali Wang, Martin Neil, and Norman Fenton. "A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model". In: *Computers & Security* 89 (2020), p. 101659.
- [95] Willis Ware et al. *Security controls for computer systems*. Report of Defense Science Board Task Force on Computer Security. Rand Corporation, 1970.
- [96] Muhammad Yasin, Arry Akhmad Arman, Ian Joseph M. Edward, and Wervyan Shalannanda. "Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)". In: *2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*. 2020, pp. 1–5. DOI: 10.1109/TSSA51342.2020.9310875.

APPENDIX 1 CONTROL SELECTION USING AI

To test how current AI platforms respond to different questions and provide suggestions to select the 10 most important information security controls in priority order, the question is amended with the addition of the organizational priorities of CIA properties and the addition of the minimal resources of the organization. Based on the additions, eight questions are formed to be asked from by AI chat interfaces:

- Q1. What are in priority order the ten most important information security controls for SMEs?
- Q2. What are in priority order the ten most important information security controls for SMEs having minimal resources?
- Q3. What are in priority order the ten most important information security controls for SMEs who prefer high information confidentiality?
- Q4. What are in priority order the ten most important information security controls for SMEs who prefer high information confidentiality but have minimal resources?
- Q5. What are in priority order the ten most important information security controls for SMEs who prefer high information availability?
- Q6. What are in priority order the ten most important information security controls for SMEs who prefer high information availability but have minimal resources?
- Q7. What are in priority order ten most important information security controls for SMEs who prefer high information integrity?
- Q8. What are in priority order the ten most important information security controls for SMEs who prefer high information integrity but have minimal resources?

The results of the questions are presented in the following tables. The first column indicates the suggested control name, and the priority order for the control is in the column of each question. Controls have been combined in the response if the content of the control is similar and even the control name would not have been an exact match.

The following Table 7 contains results of ChatGPT 3.5, and Table 8, the results of Copilot. In Copilot's settings, the response style was set to exact.

TABLE 8 Copilot's responses to questions

Control	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Asset management	1	7	3	3	5		3	3
Policies, standards, and guidelines	2		10		10		10	
Incident management	3	9	4	4	4	4	4	4
Access control management	4	8	1	1	6		1	1
Network security and data exchanges	5		2	2	3	3	2	2
Vulnerability management	6		5		7		5	
Fighting malware	7		6		8		6	
Backup management	8	10	7		2	2	7	
Safeguards management	9		8		9		8	
ICT readiness for business continuity	10		9		1	1	9	
Develop good cybersecurity culture		1		5		5		5
Publish cybersecurity policies		2		6		6		6
Conduct cybersecurity audits		3		7		7		7
Remember data protection		4		8		8		8
Provide appropriate training		5		9		9		9
Ensure effective third-party management		6		10		10		10

ORIGINAL PAPERS

I

INFORMATION SECURITY MANAGEMENT SYSTEM STANDARDS: A GAP ANALYSIS OF THE RISK MANAGEMENT IN ISO 27001 AND KATAKRI

by

Riku Nykänen & Mikko Hakuli 2013

Proceedings of the 12th European Conference on Information Warfare and
Security, ECIW 2013, 344-350

Reproduced with kind permission of Academic Conferences.

Information Security Management System Standards: A Gap Analysis of the Risk Management in ISO 27001 and KATAKRI

Riku Nykänen, Mikko Hakuli
University of Jyväskylä, Jyväskylä, Finland
riku.t.nykanen@student.jyu.fi
mikko.s.hakuli@student.jyu.fi

Abstract: An information security management system (ISMS) provides controls to protect organizations their most fundamental asset, information. Risk management is an essential part of any ISMS. ISO27001 is a widely adopted ISMS standard that sets specific information security requirements for the management system. Organizations that claim to have adopted ISO27001 can be formally audited and certified to comply with the ISO27001 standard. KATAKRI is a Finnish national security auditing criteria that is based on several ISMS standards and best practices. It was initially intended to be used by public sector to audit private sector service providers, but it has been adopted also as a baseline of requirements for private sector security standards. Since many organizations have claimed ISO27001 certification, it is beneficial to analyse the gaps between ISO 27001 and national KATAKRI certifications. This paper explores structures of ISO 27001 and KATAKRI and presents results of gap analysis of risk management requirements between ISO 27001 controls for information security management and KATAKRI requirements.

Keywords: information security management system (ISMS), risk management, ISO 27001, KATAKRI

1. Introduction

Risk management is an essential part of all major information security management systems. One of the key objectives of risk management is to identify and secure key assets to enable business operations and their continuity. The information technology causes a number of risks in performing operational activities and these risks are expected to continue to escalate as new technologies emerge (Pereira and Santos, 2010).

Information security helps to mitigate the various risks through the application of a suitable range of security controls (Posthumus and von Solms, 2004). Each industry operates in different risk environment. In addition to common risks each organization has its own unique risks. Hence organizations continuously struggle to choose and implement the cost efficient set of security controls that mitigates the risks to acceptable level. (Baker and Wallace, 2007)

Many organizations apply certification for their ISMS to convince their stakeholders that security of organization is properly managed and meets regulatory security requirements (Broderick, 2006). Security aware customers may require ISMS certification before business relationship is established (KATAKRI, 2011). As there is a variety of different ISMS approaches available, organizations may even be requested to have multiple certifications.

ISMS standards are not the silver bullet and they possess potential problems. Usually guidelines are developed using generic or universal models that may not be applicable for all organizations. Guidelines based to common, traditional practices take into consideration differences of the organizations and organization specific security requirements. (Siponen and Willison, 2009)

In this study we compare the internationally widely used ISO/IEC 27001 to Finnish national ISMS approach called KATAKRI. Comparison is limited to risk management requirements of ISMS. The paper is structured as follows: in the section 2 an overview of risk management as part of ISMS and overview of selected standards are presented. In section 3 we briefly present need for gap analysis and present a model of how the requirements were divided into phases for analysis; section 4 presents summary of the results of the gap analysis; conclusions of the results of the gap analysis are presented in section 5; discussion and future work are presented in section 6.

2. Risk management as part of information security management

2.1 Risk components in security ontology

Area of security involves people with different roles within organizations. This emphasizes the role of common understanding of the used terminology. Comprehensive study of security ontologies (Blanco et al., 2011) denotes that security community, including risk analysis community, lacks common ontology thus there exist many domain specific ontology definitions.

Risk components should be identified in Certification and Accreditation (C&A) process requiring risk management (Gandhi and Lee, 2007). ISO/IEC definitions are commonly used for terms asset, vulnerability, threat and control. Assets are something having value for the organization and what needs to be protected. Countermeasures can mitigate or reduce vulnerabilities to acceptable level. Control (countermeasure) is a mean of managing risk, including policies, procedures, guidelines, practices or organizational structures. Threat a potential cause of an unwanted incident, which may result in harm to a system or organization. Vulnerability is a weakness of an asset or group of assets that can be exploited by threats. (ISO/IEC 27002) In this paper we use previous ISO/IEC definitions unless otherwise stated.

2.2 Definition of requirements for ISMS

Desirable and “complete” security requirements cover seven facets: who, where, what, when, why, which and how? Structured requirement definitions with well-designed requirement attributes provide clearer, concise, and informative requirements compared to natural language requirement definition. (Lee et al., 2006)

C&A requirements are generally written in natural language instead of structured requirements (Gandhi and Lee, 2007). According to Lee et al. (2006) natural language requirements suffer from range of problems related to, for example, consistency, completeness and redundancy. Natural language requirements are often long and verbose, but decomposing a requirement may change the meaning or context of the requirement. However, decompositions ease requirement compliance evaluation. Another problem is varying requirement abstraction levels. Decomposition and restructuring is a solution for this problem also. The third addressed problem in the natural language requirements is that requirements suit to multiple requirement categories. The last of the presented problems is having redundant requirements. The same requirement may be expressed even within same document using different terminologies.

2.3 ISO/IEC 27000 standards family

ISO/IEC 27001 is an information security standard published by the ISO/IEC standardization organization in 2005. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System. ISO/IEC 27001 specifies requirements for the management of the implementation of the security controls. The controls and implementation guidelines than an organization may use are presented in ISO/IEC 27002. Controls represented in appendix of ISO/IEC 27001 and in ISO/IEC 27002 are normative. Organization defines which of the controls it shall implement. Organization may request certification against ISO/IEC 27001 for implemented ISMS. ISO/IEC 27001 contains definition of the term and definitions. Definitions refer to other ISO/IEC standard documents. Hence all ISO/IEC 27000 family standards share a common ontology.

ISO/IEC 27001 describes four-phase cyclic process known as “Plan-Do-Act-Check” (PDCA).

- Plan: establish security policy, objectives, processes and procedures.
- Do: implement the security policy and relevant procedures.
- Check: assess and measure the process performance.
- Act: take corrective and preventive actions.

Applying PDCA model, organization adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS. ISO/IEC 27000 Information Security Management System standards family includes also ISO/IEC 27005 standard for risk management. Its purpose is equal to ISO/IEC 27002 as it provides implementation guidance that can be used when planning risk management activities.

Boehmer (2009) claims that ISMS based on ISO 27001 is equivalent to risk management, which again is equivalent cost/benefit management. Risk approach is in the interest of organizations that want to avoid wasting investments in information security, and to find cost-efficient, risk mitigating controls.

2.4 KATAKRI – Finnish national security auditing criteria

Another approach to manage corporate security is Finnish national security auditing criteria, KATAKRI. It is published by the ministry of defence, but Confederation of Finnish Industries, Finnish Communications Regulatory Authority, ministry of foreign affairs and ministry of the interior have also participated in the preparation of the criteria. Initial version was published in 2009 and the updated version II in 2011.

The first goal of national security auditing criteria is to harmonize official measures while assessing organization security level. The second defined goal is “to support companies and other organizations as well as authorities with their service providers and subcontractors to work on their own internal security”. Therefore criteria contain unofficial recommendations to help users to apply useful security practices. (KATAKRI, 2011)

KATAKRI is organized as requirements compliance questionnaire. It defines a number of requirements in form of questions. Each question consists of a tripartite classification of criteria, corresponding to the security level concepts: the base level (level IV), the increased level (level III) and the high level (level II). For KATAKRI certification the organization shall select the pursued security level. Based on selection, every criterion defined for the selected security level must be complied in each question. The questions and criteria are defined in natural language.

Criteria are divided into four main areas:

- administrative security
- personnel security
- physical security
- information security

Areas are not meant to be used independently. It is instructed to take all four areas into account when performing accreditation audit using KATAKRI. (KATAKRI, 2011)

KATAKRI does not include definition of terminology that is used. Each question contains, in addition to requirements to all security levels, two columns; “recommendations for the industry” and “source/additional information”. For the questions having sources defined, definitions of terms can be derived from defined requirement sources. Lack of the common ontology can be seen as major weakness of KATAKRI compared to other ISMS standards.

3. Risk management compliance gap analysis

In this research we focus on ISO/IEC 27001 and KATAKRI risk management requirements. Organization may request certification for implemented ISMS against both standards. They both define their own specific set of requirements that ISMS must fulfill to be compliant.

In the preface of KATAKRI it is stated that “the criteria have been created from the perspective of absolute requirements and they do not include a marking system which is used in some criteria”. Also, ISO/IEC 27001 states that “excluding any of the requirements specified in Clauses 4, 5, 6, 7, and 8 is not acceptable when an organization claims conformity to this International Standard.” As both approaches present absolute prerequisite to meet all requirements with yes/no satisfaction criteria, results are comparable by comparing requirements as results are in same scale. Both KATAKRI and ISO/IEC 27001 use the scale of being full compliance or non-compliance. Partial compliance is not accepted. As Karabacak and Sogukpinar (2006) state that the official certification can be difficult as it is “all-or-nothing” design.

The main research question was to analyze is the ISO/IEC audited risk management process compliant with KATAKRI requirement for risk management. Analysis method was selected to support

bidirectional analysis to see compliance to both of the directions. As result of the analysis we expected to see gap analysis of risk management requirements of ISO/IEC 27001 and KATAKRI. We hope to see that results of this analysis will help organization having either of the certifications to evaluate easier amount of actions required to pursue the other certification.

The risk management requirements are covered in ISO/IEC 27001 in section 4.2.1. There are six main requirements. Three of these requirements contain ten more specific requirements for the corresponding main requirements.

In KATAKRI, risk management requirements are covered in the first part, administrative security. In this part there is subdivision A400, "Identifying, assessing, and controlling risks". This part contains 12 questions, which each contain several requirements. Risk management requirements are not only limited to section A400, but there are risk management requirements also in other subdivisions of the administrative security main part.

Fenz and Ekelhart (2011) have analyzed five commonly used ISRM methodologies and derived a generic ISRM view out of the selected methodologies. They have created five phases for risk management. Phases and their outputs are represented in table 1.

Table 1: Information security risk management phases and their outputs by Fenz and Ekelhart (2011).

ISRM phases and outputs	
Phase	Output
System characterization	Inventory list of assets to be protected, including their acceptable risk level.
Threat and vulnerability assessment	List of threats and corresponding vulnerabilities endangering the identified assets.
Risk determination	Quantitative or qualitative risk figures and levels for identified threats.
Control identification	List of potential controls that can mitigate the risks to an acceptable level.
Control evaluation and implementation	List of cost-efficient controls that have to be implemented to reduce the risk to an acceptable level.

We identified the risk management requirements from ISO/IEC 27001 and KATAKRI and categorized them into ISRM phases. Content of each category was analysed to find gaps between requirement definitions. Both ISO/IEC 27001 and KATAKRI define requirements to establish risk assessment procedure, which is outside of the scope of ISRM phases. Hence these requirements were analysed as separate set of requirements.

4. Results

This chapter represents key results of the requirement analysis. In the following tables 2 and 3, requirement criteria without corresponding criteria in other specification is presented in *italic* style. Tables don't include all requirements for clarity, but the most important requirements for all phases are included.

Requirements outside of the scope of ISRM phases set the prerequisites to implement risk assessment methodology, which shall implement requirements categorized into phases. Table 2 represents identified requirements for risk assessment procedures.

Table 2: Risk assessment procedure requirements mapping

Risk assessment procedure requirements mapping	
KATAKRI	ISO/IEC 27001
<ul style="list-style-type: none"> • Define a risk assessment procedure (A401.0) • Results of the risk assessment procedure are documented (A401.0) • <i>Measure risk assessment process (A407.0)</i> • <i>Risk assessment is performed annually or when significant changes occur (A403/level III) or risk assessment is part of management process (A403/level II)</i> • <i>Results of risk assessment are considered when setting goals of the security work (A404.0)</i> 	<ul style="list-style-type: none"> • Identify a risk assessment methodology suited to requirements (4.2.1c1) • Develop criteria for accepting risks (4.2.1c2)

Identified risk management requirements from ISO/IEC 27001 and KATAKRI were mapped to the presented ISRM phases. Results of the mapping are presented in table 3. Corresponding security level is presented in KATAKRI requirements. In addition table includes ISO/IEC 27005 mapping (Fenz 2011).

Table 3: Information security risk management phase mapping

Information security risk management phase mapping			
Phase	KATAKRI	ISO/IEC 27001	ISO/IEC 27005 (Fenz 2011)
System characterization	<ul style="list-style-type: none"> • Asset identification (A401.1) • Identify owners of assets (A401.1) 	<ul style="list-style-type: none"> • Identify acceptable levels of risk (4.2.1c2) • Asset identification (4.2.1d1) • Identify owners of assets (4.2.1d1) 	<ul style="list-style-type: none"> • Asset identification
Threat and vulnerability assessment	<ul style="list-style-type: none"> • Threat assessment (A401.1) • Identify vulnerabilities (I706.0) 	<ul style="list-style-type: none"> • Identify threats (4.2.1d2) • Identify vulnerabilities (4.2.1d3) 	<ul style="list-style-type: none"> • Identify threats • Identify vulnerabilities
Risk determination	<ul style="list-style-type: none"> • Assess risks (A401.2) • Risks are prioritised (A405.0) • Likelihood risk estimation (A405.0/level II) • Risk assessment covers at least security management and personnel, information and premises security (A402.0) • <i>Risks relating to external actors are identified (A402.0, A409.0)</i> • <i>Risk assessment influences to security training (A405.0)</i> 	<ul style="list-style-type: none"> • Identify impact (4.2.1d4, 4.2.1e1) • Assess threat likelihood (4.2.1e2) • Assess vulnerability (4.2.1e2) • Likelihood risk estimation (4.2.1e4) 	<ul style="list-style-type: none"> • Identify impact • Assess threat likelihood • Assess vulnerability • Likelihood risk estimation

Control identification	(No requirements)	<ul style="list-style-type: none"> • <i>Identify and evaluate options for the treatment of risks (4.2.1f)</i> 	<ul style="list-style-type: none"> • Evaluate existing and planned controls
Control evaluation and implementation	<ul style="list-style-type: none"> • Controls are proportioned to the assets and the relevant risks (A401.1) • Management approved chosen controls (A401.2) • Management approval for residual risks (A401.2) 	<ul style="list-style-type: none"> • Select control objectives and controls (4.2.1g) • Management approval for residual risks (4.2.1h) 	<ul style="list-style-type: none"> • Information security risk treatment (risk avoidance, risk transfer, risk reduction, or risk retention)

As seen from table, KATAKRI does not explicitly require identify and evaluate possible options to mitigate the risks. Rationale for this can be found from the other sections of KATAKRI documentation. Criteria itself contains mandatory controls for each defined security level. Therefore it is not mandatory for organization to evaluate other possible risk treatment options or controls. As ISO/IEC 27001 does not set any specific controls, but only defines normative controls, it is mandatory for organization itself to identify and evaluate appropriate options for risk treatment.

5. Conclusions

Comparing natural language requirements has exposed variety of problems. Many of the analyzed requirements have problems with the completeness. KATAKRI also contains several redundant requirements. Mutual ontology between compared standards facilitates analysis. While KATAKRI is lacking definition of terms, its definitions must be extracted from referred documents. In subdivision A400, "Identifying, assessing, and controlling risks" both ISO/IEC 27001 and 27002 are among the referred documents. Hence risk management terminology is coherent in both documents, but problems exist in other parts of the KATAKRI.

Gap analysis indicates that the KATAKRI certified ISMS implements the most of the risk management requirements of ISO/IEC 27001, but some exceptions exist. As presented in previous chapter, KATAKRI does not have requirement to evaluate and identify possible options for risk treatment. Rationale for this is that KATAKRI itself defines minimum set of controls for each defined security level. ISO/IEC 27001 does not define any mandatory controls, but all controls defined in ISO/IEC 27002 are under considered as normative. The second ISO/IEC 27001 requirement missing from KATAKRI is risk likelihood analysis, which is required by the KATAKRI only on the high security level (level II). KATAKRI requires grouping risks by the importance, but this is not exactly same requirement as likelihood analysis, because risk importance may comprise other risk attributes such as impact. The third difference is the identification of the vulnerabilities. KATAKRI does not require risk management process to identify vulnerabilities, but has requirement to identify the technical vulnerabilities in section of information assurance.

ISO/IEC 27001 certified ISMS does not automatically fulfill all KATAKRI risk management requirements. Following requirements from KATAKRI are not included in ISO/IEC 27001:

1. Risk management process is measured.
2. Risk assessment is performed annually or when significant changes occur (A403/level III) or risk assessment is part of management process (A403/level II).
3. Risk assessment results drive security work.
4. Management has approved chosen controls.
5. Risk assessment is also required, when relevant, from external actors like subcontractors and service providers.
6. Risk assessment influences to security training.

When organization implements ISMS using PDCA model, the requirements for measurement, periodic assessment, results driving security work and management approval for security controls, should be

fulfilled. These are part of “check” and “act” phases of PDCA model to measure results and achieve continuous improvement of ISMS.

The other two deviating requirements, “assessing external parties” and “assessment influence to security training” are covered by normative controls in ISO/IEC 27002. Requirement assessing external parties is analogous to “Addressing security in third party agreements”. In ISO/IEC 27002, control “Information security awareness, education, and training” has guideline to include known threats in security training. If this control is implemented, ISMS procedure should also fulfill the KATAKRI requirement.

In this study our target was to compare contents of risk management requirements between ISO/IEC 27001 and KATAKRI. As results show, some deviations between requirements exist in both directions and requirements are not completely overlapping. Major deviation between models is the identification of possible options for the risk treatment. Where ISO/IEC 27001 requires organizations to implement a process to identify potential options, KATAKRI defines itself a minimum set of controls for each of the three security levels. Most of the KATAKRI requirements missing from ISO/IEC 27001 are fulfilled when ISMS is implemented using PDCA model. Other deviations in the risk management are minor and a well implemented ISMS should cover these requirements.

6. Discussion

This research was limited to analyzing KATAKRI and ISO/IEC 27001 requirements for risk management. For organizations having either of certifications, it would be meaningful to have analysis of complete requirement definitions. Comparison structure should compare each security level from KATAKRI to combination of ISO/IEC 27001 and 27002. As we have seen that some of the KATAKRI requirements are covered in the normative controls of ISO/IEC 27002, which should be included in comparison even if it is a normative document.

In this study we have identified some problems that KATAKRI currently comprises. One of them is the lack of common ontology over the document. This leaves possibility for interpretation instead of having exact requirements for ISMS. Another identified problem is the natural language requirements. As long as KATAKRI is structured as requirements compliance questionnaire, the problem can only be mitigated by enhancing requirement definition quality.

Future research is continued on evaluating existing risks for IT companies and how current ISMS certification models correlate to existing risks. One of the goals is to study if the ISMS certificate will help organizations to find cost-efficient, risk-reducing security controls or does certification just cause additional costs for the organization that doesn't reduce actual risks at all.

References

- Baker, W.H. & Wallace, L. 2007, "Is Information Security Under Control?: Investigating Quality in Information Security Management", *Security & Privacy, IEEE*, vol. 5, no. 1, pp. 36-44.
- Blanco, C., Lasheras, J., Fernández-Medina, E., Valencia-García, R. & Toval, A. 2011, "Basis for an integrated security ontology according to a systematic review of existing proposals", *Computer Standards & Interfaces*, vol. 33, no. 4, pp. 372-388.
- Boehmer, W. 2009, "Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001", *Availability, Reliability and Security, 2009. ARES '09. International Conference on*, pp. 392.
- Broderick, J.S. 2006, "ISMS, security standards and security regulations", *Information Security Technical Report*, vol. 11, no. 1, pp. 26-31.
- Fenz, S. & Ekelhart, A. 2011, "Verification, Validation, and Evaluation in Information Security Risk Management", *Security & Privacy, IEEE*, vol. 9, no. 2, pp. 58-65.
- Gandhi, R.A. & Lee, S. 2007, "Discovering and Understanding Multi-dimensional Correlations among Certification Requirements with application to Risk Assessment", *Requirements Engineering Conference, 2007. RE '07. 15th IEEE International*, pp. 231.

ISO/IEC 27001:2005 2005, Information technology – Security techniques – Information security management systems – Requirements, ISO copyright office, Geneva, Switzerland.

ISO/IEC 27002:2005 2005, Information technology – Security techniques – Information security management systems – Code of practice for information security management, ISO copyright office, Geneva, Switzerland.

Karabacak, B. & Sogukpinar, I. 2006, "A quantitative method for ISO 17799 gap analysis", *Computers & Security*, vol. 25, no. 6, pp. 413-419.

KATAKRI 2011, National Security Auditing Criteria version II, Ministry of Defence, Finland.

Lee, S., Gandhi, R., Muthurajan, D., Yavagal, D. & Ahn, G. 2006, "Building problem domain ontology from security requirements in regulatory documents", *Proceedings of the 2006 international workshop on Software engineering for secure systems* ACM, New York, NY, USA, pp. 43.

Pereira, T. & Santos, H. "A Conceptual Model Approach to Manage and Audit Information Systems Security", *Proceedings of the 9th European Conference on Information Warfare and Security*, Academic Conferences Limited, pp. 360.

Posthumus, S. & von Solms, R. 2004, "A framework for the governance of information security", *Computers & Security*, vol. 23, no. 8, pp. 638-646.

Siponen, M. & Willison, R. 2009, "Information security management standards: Problems and solutions", *Information & Management*, vol. 46, no. 5, pp. 267-270.

II

COMPARISON OF TWO SPECIFICATIONS TO FULFILL SECURITY CONTROL OBJECTIVES

by

Riku Nykänen & Tommi Kärkkäinen 2014

Proceedings of the 13th European Conference on Cyber Warfare and Security,
ECCWS-2014, 150-159

Reproduced with kind permission of Academic Conferences.

Comparison of two specifications to fulfill security control objectives

Riku Nykänen, Tommi Kärkkäinen
University of Jyväskylä, Jyväskylä, Finland
riku.t.nykanen@student.jyu.fi
tommi.karkkainen@jyu.fi

Abstract: Assuring information security is a necessity in modern organizations. Many recommendations for information security management (ISM) exist, which can be used to define baseline of information security requirements ensuring that an organization has implemented the selected practices. ISO/IEC 27001 prescribes a process for ISM system and guidance to implement security controls is provided in ISO/IEC 27002. Finnish National Security Auditing Criteria (KATAKRI) has been developed by the national authorities in Finland to verify maturity of information security practices. KATAKRI defines both security control objectives and absolute security controls to meet an objective. ISO/IEC 27001 requires selection of valid security controls whereas KATAKRI may force organization to implement controls that are not feasible from risk management or cost-benefit ratio point of view. In our work, we study differences of the security control objectives and the actual controls of ISO/IEC 27002 and KATAKRI to analyze completeness and mutual coverage between the two specifications. The results reveal the different scope and the lack of some of the controls of KATAKRI compared to ISO/IEC 27001 and ISO/IEC 27002.

Keywords: information security management, ISO/IEC 27001, ISO/IEC 27002, KATAKRI

1. Introduction

Assuring information security is a necessity in modern organizations. There exists variation of viewpoints in information security management (ISM) concerning 'what' should be done (ISO/IEC 27000 and COBIT; IT management), 'how' it should be done (ITIL; service management), and 'who' should do it (SFIA; competence management), see (Armstrong 2013). These recommendations are used to define baseline of information security requirements ensuring that an organization has implemented the selected practices. Some of the recommendations provide the possibility for organizations to request certification, which is can then be granted if the implemented practices fulfill the audition criteria.

Widely adopted ISO/IEC 27001 prescribes a process for ISM system whereas guidance to implement security controls is defined in ISO/IEC 27002. Hence, together they comprise minimum criteria of controls and their objectives, providing also non-normative guidance for control implementation. Finnish National Security Auditing Criteria (KATAKRI) has been developed by the national authorities in Finland to verify maturity of information security practices. Approach in KATAKRI is different compared to ISO/IEC 27000 standards. As national security auditing criteria, KATAKRI defines both security control objectives and absolute security controls to meet an objective. Implementation of controls is mandatory whereas ISO/IEC 27001 leaves responsibility of the selection of controls and their implementation to organization itself by defining only the control objectives. Use of ISO/IEC 27001 is always subject to completeness of risk assessment and selection of valid security controls. On the other hand, KATAKRI may force organization to implement such controls that are not feasible from risk management or cost-benefit ratio point of view.

In our work, we study differences of security control objectives and actual controls of ISO/IEC 27001 and KATAKRI requirements to analyze completeness and mutual coverage of KATAKRI and ISO/IEC 27001. The actual comparison also takes into account ISO/IEC 27002 security control implementation guidelines, creating links between them and the security requirements in KATAKRI. First of all, however, the two specifications are united in their terminology and structure, but whereas ISO/IEC 27002 focuses on existence of security controls to meet the security objectives, KATAKRI defines different levels of requirements that shall be fulfilled. Barlette & Fomin (2008), Fomin et al (2008), Yeniman Yildirim et al (2011), and Siponen (2006) all criticize that information security management standards focus on security process, not how well activities are carried out or how objectives are achieved. To cope with these ISMS hindrances, we create an explicit linking between a process-oriented standards and (normal) operative mode assessment in an organization.

Our analysis of KATAKRI and ISO/IEC 27002 specifications is focused to see the amount of shared common security aspects. In addition, we are interested in differences of the specifications to see the potential gaps in them, especially in the relatively new KATAKRI.

The contents of the paper are as follows: After the introduction, we provide background information on the two specifications and comparative approach in general in Section 2. Then, in Section 3 a structural comparison of specifications and high level comparison of contents of the both specifications is provided. In Section 4, we present more detailed comparison results including intersection and complements of the specifications. In Section 5 we have discussion on the results and further research.

2. Background

2.1 Basic concepts

ISO/IEC definitions are commonly used for terms asset, vulnerability, threat, and control. Assets are something having value for the organization and what needs to be protected. Risk is a combination of the probability of an event and its consequence. Control (countermeasure) is a mean of managing risk, including policies, procedures, guidelines, practices, or organizational structures. Threat is a potential cause of an unwanted incident, which may result in harm to a system or organization. Vulnerability is a weakness of an asset or group of assets that can be exploited by threats. (ISO/IEC 27002, 2005)

2.2 ISO 27000 standards

ISO/IEC 27001 is an information security standard published by the ISO/IEC standardization organization in 2005. It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System. ISO/IEC 27001 specifies requirements for the management of the implementation of the security controls. The controls and implementation guidelines than an organization may use are presented in ISO/IEC 27002.

Appendix of ISO/IEC 27001 and ISO/IEC 27002 itself contain comprehensive list of controls and their objectives. Although ISO/IEC 27001 states that also additional control objectives and controls may be needed and identified from other sources. Organization defines which of the controls it shall implement. Organization may request certification against ISO/IEC 27001 for implemented ISMS. For both ISO/IEC 27001 and 27002 updated versions were released on October 2013.

2.3 KATAKRI – Finnish national security auditing criteria

Another approach to manage corporate security is the Finnish national security auditing criteria, KATAKRI. It is published by the Ministry of Defence, but Confederation of Finnish Industries, Finnish Communications Regulatory Authority, Ministry of Foreign Affairs, and Ministry of the Interior have also participated in the preparation of the criteria. Initial version was published in 2009 and the updated version II in 2011.

The first goal of the national security auditing criteria is to harmonize official measures while assessing organization security level. The second defined goal is “to support companies and other organizations as well as authorities with their service providers and subcontractors to work on their own internal security”. Therefore criteria contain unofficial recommendations to help users to apply useful security practices. (KATAKRI, 2011)

2.4 Comparing standards and models

Comparing standards or methodologies may reveal several hindrances. One is the lack of widely adopted common ontology containing definitions of the basic concepts and relationships. Ramanauskaite et al. (2013) have identified that major information security management standards utilize only partially comparable security ontologies. Hence, even if standards and methodologies should lead to harmonized ontology definition, there does not exist a single widely adopted ontology definition.

Pardo et al. (2011) emphasize that in comparison it is possible to, using relationships of the models, find out how different the compared models are. Pardo et al. defines that “*in the model comparison the need to know the level of equality and proportion between the things being compared should take the priority*”. One part of comparison is terminology analysis. Pardo et al (2011) divide terminology analysis into two subtypes; syntactic analysis and semantic analysis. Our study uses only semantic analysis as the contents of the compared documents is defined in natural language and require qualitative analysis.

Multiple models can have various types of connections between them. Pardo et al (2011) have identified four operations: union, intersection, difference, and complement. Intersection contains elements that are common

in all the models and union combines together the shared contents. Difference comprises elements that the compared models do not have in common. Complement is a set of elements that are not included in one of the compared models. When comparing only two models, both complements are equal to the difference of the models.

3. Structural view

From structural point of view both ISO/IEC 27001 and KATAKRI controls are divided into logical groups. Following definitions are equal in both, 2005 and 2013, ISO/IEC 27002 standard versions. In ISO/IEC 27002 standard the highest level of grouping is called clauses. Each of these clauses contain “one introductory clause introducing risk assessment and treatment” and a number of security categories. Each security category contains one control objective and one or more controls. ISO/IEC 27002:2005 defines that control objective states what is to be achieved. The security controls in the security category can be applied to achieve the control objective. Again ISO/IEC 27002 versions 2005 and 2013 state: “control defines the specific control statement to satisfy the control objective”. Each control is attached with the implementation guidance, which provides instructions on control implementation to meet the control objective. Definition of the implementation guidance also states that guidance may not be suitable for all organizations and other implementation options can be more appropriate. For each control there is also other information included such as references to other standards or legislation.

KATAKRI is organized as a requirements compliance questionnaire. It has four major sections called divisions, which are divided again into subdivisions. Each subdivision contains number of questions. It defines a number of requirements in the form of questions. Each question consists of a tripartite classification of requirements, corresponding to the security level concepts: the base level (level IV), the increased level (level III), and the high level (level II). These levels correspond to international security level concepts restricted, confidential, and secret, respectively. KATAKRI does not contain requirements for the highest security level, internationally known as top secret (level I).

For the KATAKRI certification the organization shall select the pursued security level. Based on selection, every requirement defined for the selected security level must be complied in each question. In addition to three security levels, there is additional set of requirements as recommendations for the industry. It contains useful security requirements recommended to all businesses to implement. For each level and industry recommendation, a number of requirements is attached. These requirements may be the same for all levels and industry recommendations, they may differ depending on the level, or higher security levels may add more requirements to the base level requirements. The questions and requirements are defined in natural language. For each question there is additional information, containing, for example, references to standards, including ISO/IEC 27002:2005, and implementation guidance.

Where KATAKRI requirements are merely ones that can be answered yes or no, ISO/IEC 27001 auditor has to evaluate that the identified set of security controls is comprehensive and implemented according to the qualitative requirements of the security controls.

ISO/IEC 27002 and KATAKRI both share the same approach grouping security concepts first on high level and then on the secondary level. In ISO/IEC 27002, highest level of grouping is division of security clauses. On the other hand, KATAKRI is divided into four divisions, which are further divided into subdivisions. Table 1 represents ISO/IEC 27002 security clause and the KATAKRI divisions and their subdivisions. ISO/IEC 27002 states that the security clauses are not in specific order concerning prioritization of the security clauses or controls. In KATAKRI prioritization is implemented in dividing security controls based on pursued security level, where the primary controls are defined at the base level. Hence, KATAKRI divisions and subdivisions do not relate to prioritization.

Table 1: ISO/IEC 27001 standard versions 2005 and 2013 security clauses and KATAKRI divisions and subdivisions.

Logical groups of security controls		
ISO/IEC 27001:2005	ISO/IEC 27001:2013	KATAKRI
1. Security policy	1. Information security policies	1. Administrative security
2. Organization of information security	2. Organization of information security	1.1. Security policy, the measures guiding security action and definitions
3. Asset		1.2. The annual security action programme
		1.3. Defining the goals of security

<ul style="list-style-type: none"> 4. Human resources security 5. Physical and environmental security 6. Communications and operations management 7. Access control 8. Information systems acquisition, development and maintenance 9. Information security incident management 10. Business continuity management 11. Compliance 	<ul style="list-style-type: none"> 3. Human resource security 4. Asset management 5. Access control 6. Cryptography 7. Physical and environmental security 8. Operations security 9. Communications security 10. System acquisition, development and maintenance 11. Supplier relationships 12. Information security incident management 13. Information security aspects of business continuity management 14. Compliance 	<ul style="list-style-type: none"> 1.4. Identifying, assessing and controlling risks 1.5. Security organisation and responsibilities 1.6. Accidents, danger situations, security incidents and preventive measures 1.7. Security documentation and its management 1.8. Security training, increasing awareness and knowhow 1.9. Reports and inspections by the management 2. Personnel Security <ul style="list-style-type: none"> 2.1. Technical criteria 2.2. Securing sufficient competences 2.3. Other suitability of the candidate for the task 2.4. Measures after the decision to recruit 2.5. Measures for concluding the contract of employment 2.6. Measures during employment 3. Physical Security <ul style="list-style-type: none"> 3.1. Security of area 3.2. Structural security 3.3. Security technical systems 4. Information assurance <ul style="list-style-type: none"> 4.1. Data Communications Security 4.2. Security of Information Systems 4.3. Security of Information 4.4. Security of Information Handling
---	--	--

UML class diagram of the structures of the both documents is presented in the Figure 1. ISO 27002 standards structure is equal in both version of the standard and it contains definition of terms and their relationships. KATAKRI, on the other hand, does not contain ontology definition at all. Hence, we identified basic structures of the KATAKRI document.

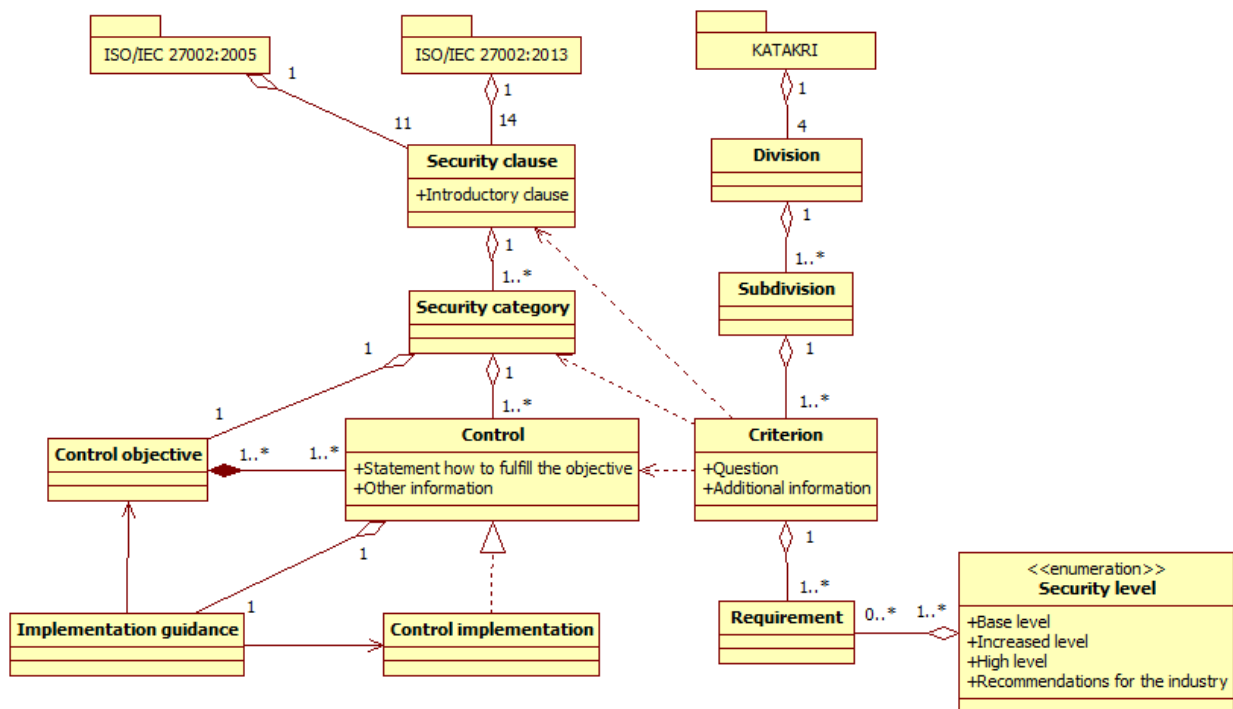


Figure 1: UML class diagram presenting structures of ISO/IEC 27002 and KATAKRI

Even if ISO/IEC 27002 and KATAKRI both share the same approach of grouping security concepts on high level, the actual structures have significant differences at lower levels. ISO/IEC 27002 standard defines control objective, which shall be achieved by implementing the defined controls. KATAKRI, on the other hand, has a question that is answered, fulfilling requirements defined for the question of the corresponding security level. Hence, KATAKRI question and ISO/IEC 27002 control objective both set goal, which is achieved by implementing defined controls or requirements.

ISO/IEC 27002 contains implementation guidance for each control that it defines. Actual implementation of the control can be done as specified in the implementation guidance or organization can select an approach that suits to its needs and characteristics (ISO/IEC 27002:2013). KATAKRI does not contain implementation guidance but provides additional information such as references to standards, legislation, and security guides.

We analyzed all requirements of the KATAKRI and identified matching definitions from ISO/IEC 27002:2005. In addition we also counted number of references from KATAKRI to ISO/IEC 27002:2005. As KATAKRI defines also requirements for risk management, we included risk management requirements of ISO/IEC 27001:2005 in the analysis.

In general, the results reveal that KATAKRI had in total 432 connections to the ISO/IEC 27002:2005. From these connections 91 were direct references to ISO/IEC 27002:2005. One of these direct references is to security clause, 16 to security categories, and 74 to security controls. KATAKRI requirements had semantic equality with 21 controls. The most of the connections were semantic equality of KATAKRI requirements to implementation guidance, which we identified 320. In addition, we found out 20 connections from KATAKRI requirements to risk management section of ISO/IEC 27002:2005 and risk management requirements in ISO/IEC 27001:2005. Hence total number of identified connections was 452. Summary matrix of the connections between ISO/IEC 27002:2005 security clauses and the KATAKRI divisions is included in the appendix 7.1 and Figure 2.

4. Operational view

We have divided the more specific results into four groups. First we present intersection of the two specifications. These are security controls that exist in both documents. Then we present complements of both ISO/IEC 27002 and KATAKRI, which discloses differences of the documents. More precisely, Section 4.2 contains security topics that are contained in ISO/IEC 27002 but not in KATAKRI and Section 4.3 contains the ones that are in KATAKRI but not in ISO/IEC 27002. We close the section by presenting other findings from the documents.

4.1 Intersection of specifications

In the general documents have sections that contain same topics, which can be seen as high number of links between security clauses and KATAKRI divisions as presented in the Figure 2: Number of connections between ISO/IEC 27002:2005 security clauses and KATAKRI divisions. Numbering is as presented in Table 1, not as security clauses are numbered according chapters in ISO/IEC 27002:2005 specification. The general security management in ISO/IEC 27002:2005 as defined in the security clauses (1-4) and (10-11) is strongly linked to KATAKRI's first division 'Administrative security'. Similarly, 'Personnel security' in KATAKRI and 'Human resource security' in ISO/IEC 27002:2005 are linked but not very strongly. Also the areas of physical security (6 in ISO/IEC 27002:2005 and 3 in KATAKRI) are connected. The fourth division, 'Information assurance' in KATAKRI is much dispersed related to ISO/IEC 27002:2005 covering both concrete areas in security operations (6-9) as well as higher level operations management (11-12).

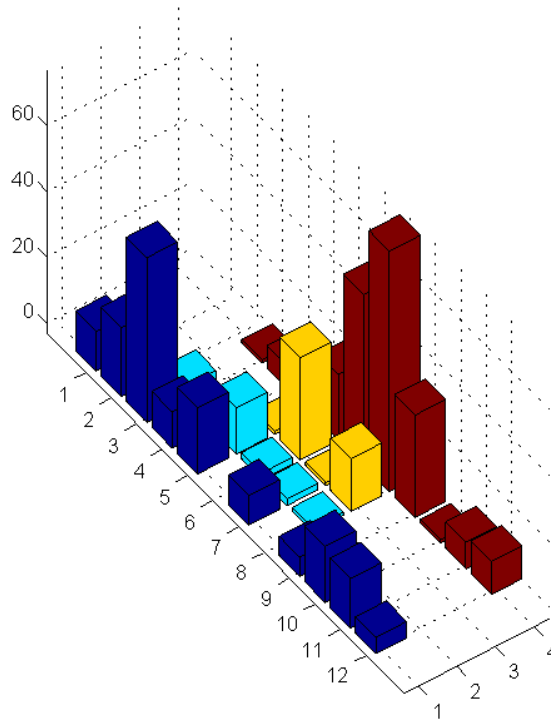


Figure 2: Number of connections between ISO/IEC 27002:2005 security clauses and KATAKRI divisions.

In detail, several common topics that were covered by both ISO/IEC 27002 and KATAKRI were identified. Following Table 2: Intersection of ISO/IEC 27002 and KATAKRI presents intersection of the specifications divided into four domains defined by the KATAKRI.

Table 2: Intersection of ISO/IEC 27002 and KATAKRI

Common topics of information security in ISO/IEC 27002 and KATAKRI	
	Common topics
Administrative security	<ul style="list-style-type: none"> • Security policy (22 connections) • Risk management (52 connections) • Security organization and responsibilities (26 connections) • Incident management (8 connections) • Business continuity management (32 connections)
Personnel security	<ul style="list-style-type: none"> • Security training (36 connections) • Contracts with employee (8 connections) • Termination of contract (6 connections)
Physical security	<ul style="list-style-type: none"> • Structural security (19 connections) • Physical access control (26 connections)
Information security	<ul style="list-style-type: none"> • Communication security (31 connections) • Information access control (26 connections) • Malware prevention and vulnerability management (12 connections) • Logging (10 connections) • Unauthorized devices (7 connections) • Encryption (6 connections) • Security of executable code (9 connections) • Handling of classified information (24 connections) • Systems management (10 connections) • Remote work/teleworking (28 connections) • Separation of production and development environments (8 connections) • Backup (10 connections)

The highest number of connections was in risk management as both methods require same approach to identify assets and threats to assets to perform risk mitigation. Both specifications keep security training and rising of the security awareness as an important aspect of information security.

4.2 ISO/IEC 27002 complements

We identified that KATAKRI contained in total only nine connections to ISO/IEC 27002:2005 security categories “12.1 Security requirements of information systems” and “12.2 Correct processing in applications”. These two security categories contain requirements for new information system development and only nine links is relatively small amount to cover all requirements for the information system development. In the ISO/IEC 27002:2013 “12.1 Security requirements of the information systems” has been updated and category number has been changed to 14.1. Section “12.2 Correct processing in applications” and controls of it in ISO/IEC 27002:2005 have been removed from version 2013. These have been complemented with two new controls in section 14.1 of the 2013 version, but KATAKRI don't have wider correlation to either of these. Rationale for this is that KATAKRI is not meant to provide requirements for information system development, because it is audition criteria. Actually a security guideline for information system development in the state institutions, called “VAHTI 1/2013 Sovelluskehityksen tietoturvaohje”, has been published. This guideline covers security requirements for the information system development. Problem has been identified also in Finnish Defence Forces in the thesis by Liitsalo (2013) where she concludes that VAHTI 1/2013 has fulfilled the lack of common national guideline of generic information system development security requirements.

ISO/IEC 27002:2005 contains one security category, “10.9 Electronic commerce services”, where we did not identify any links from KATAKRI. This category and contained controls have been removed from ISO/IEC 27002:2013. At the time ISO/IEC 27002:2005 was published electronic commerce was emerging and it was seen as an important domain to cover. As time passed, there are many other information systems available through the internet. Hence, electronic commerce services have become only a one type among other services provided in internet, which all need to consider security in the cyber age.

ISO/IEC 27002:2013 contains controls to gather evidence in case of security incident. In KATAKRI one finds very limited requirements to cover evidence collection in case of security incidents. The KATAKRI requirements merely focus to protect audit trails, but don't include additional requirements to collect and secure the evidence.

Further complementing area in ISO/IEC 27002, compared to KATAKRI, was reporting of security weaknesses. The ISO/IEC 27002 has a specific control (13.1.1 in version 2005 and 16.1.3 in version 2013) to emphasize employee responsibility report observed or suspected security weaknesses and vulnerabilities. KATAKRI does not contain requirement that would highlight employee responsibility to report weaknesses, even if it clearly states that for each employee the security responsibilities must be defined in their job description.

The compliance was an area where the level of details varied between specifications. Where ISO/IEC 27002 provides implementation instructions types for compliance and how to achieve compliance, KATAKRI has only the basic requirement that all operations must be compliant according to legislation.

4.3 KATAKRI complements

KATAKRI has some topics that are not part of ISO/IEC 27002 standards. On the administrative security KATAKRI contains the concept of annual security action programme, which is covered in KATAKRI subdivision A200. It is an annual plan how security will be developed comprising measures, responsibilities, schedules, and measurable results. The results of the implementation of the plan are expected to be monitored by the management as continuous process. It is notable that there are no requirements for annual security programme at the base level, but they are included in the recommendations for the industry.

We identified number of requirements in KATAKRI that require documentation of the performed actions, but did not find equal control from ISO/IEC 27002 control objective or implementation guidance. One such topic was training, where KATAKRI requirement define that the arranged trainings must be documented, including training material and participants. ISO/IEC 27002 controls have similar control to raise awareness, but implementation guidance does not cover documentation of training. Similar widely used documentation requirement was is a job description, which is in several KATAKRI requirements referred as written definition of the responsibilities of an employee.

KATAKRI complements ISO/IEC 27002 on high security requirements. KATAKRI contains requirements that must be fulfilled to be able to handle material that is classified secret by the Finnish national definition. For the organizations that don't consider information security as competitive advantage, these controls may not be feasible to implement. These controls don't have high cost-benefit-ratio and are valid only in security critical businesses.

Hence, KATAKRI is Finnish national security audition criteria and it contains also requirements that may be illegal in other countries. Such requirements are drug tests and probationary period used in recruitment. KATAKRI also contains national requirements for physical security alarms. Such requirements are not included in the ISO/IEC 27002 standard.

4.4 Additional results

We found out also more than 20 major translation errors in KATAKRI (original version is in Finnish, which is translated to English), where a translation error caused difference in requirements. For example, in some criterions there was for certain security level "No requirements" in English version, but the original Finnish version did contain requirements.

5. Discussion

In our study we analyzed ISO/IEC 27002 versions 2005 and 2013 and compared them to Finnish security audition criteria, KATAKRI. We found out that both contain largely same security controls that security aware organizations should implement, but under a completely different structural division. Analysis also illustrates evolution of information security management trends. Results can be applied in upcoming versions of KATAKRI to evaluate the overall scope and boundaries of the security controls. They are equally relevant for ISO/IEC standardization, even if a refined version already appeared in 2013.

We identified number of common security topics that we covered by the both of the specifications. The results reveal the different scope and lack of some of the controls of KATAKRI compared to ISO/IEC 27001 and ISO/IEC 27002. Moreover, normative controls of the KATAKRI were detected, which are not included even as implementation guidance in ISO/IEC 27002.

It has been noticed that SMEs have to focus more on development of their information security procedures, but most of the ISMS standards are not usable from SME organization point of view. For example, ISO/IEC 27001 has been criticized being too large and complicated to be adopted with the resources of SMEs. While SMEs struggle with limited resources, but increasing threads, it is important to develop new approaches that suit especially for SMEs. Majority of modern information security management systems are developed for at least medium sized enterprises. One question driving our future study is: "we have firewall and antivirus software, but what next?"

KATAKRI contains basic prioritization of the security requirements as all the requirements have been defined for three information classification levels and in addition there are recommendations for the industry. ISO/IEC 27002 in the other hand states in the document that security controls are not in any means prioritized. In the KATAKRI, even at the lowest security level (or only even the recommendations for the industry), amount of controls is out reach for SMEs where security is not strategic competence area. For example, the NIST standard 800-53 (2009) defining recommended security controls for the federal information systems and organizations, contains prioritization of the security controls.

In addition we plan to include viewpoints for organization types and personnel roles to security tools. Where current document-based approaches are rigid to separate interesting topics of different job functions, some modern presentation methods, like wiki-format, may be more usable.

6. References

Armstrong, C.J. 2013, "An Approach to Visualising Information Security Knowledge" in *Information Assurance and Security Education and Training*, Springer Berlin Heidelberg, pp. 148-155.

Barlette, Y. & Fomin, V.V. 2008, "Exploring the Suitability of IS Security Management Standards for SMEs", *Hawaii International Conference on System Sciences*, Proceedings of the 41st Annual, pp. 308.

Fomin, V.V., de Vries, H.J. & Barlette, Y. 2008, "ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption", *EUROMOT 2008 Conference*, Nice, France.

ISO/IEC 27001:2005 2005, *Information technology - Security techniques - Information security management systems - Requirements*, ISO copyright office, Geneva, Switzerland.

ISO/IEC 27001:2013 2013, *Information technology - Security techniques - Information security management systems - Requirements*, ISO copyright office, Geneva, Switzerland.

ISO/IEC 27002:2005 2005, *Information technology - Security techniques - Information security management systems - Code of practice for information security management*, ISO copyright office, Geneva, Switzerland.

ISO/IEC 27002:2013 2013, *Information technology - Security techniques - Information security management systems - Code of practice for information security management*, ISO copyright office, Geneva, Switzerland.

KATAKRI 2011, *National Security Auditing Criteria version II*, Ministry of Defence, Finland.

NIST Special Publication 800-53 2009, *Recommended Security Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology.

Pardo, C., Pino, F.J., García, F., Piattini, M. & Baldassarre, M.T. 2012, "An ontology for the harmonization of multiple standards and models", *Computer Standards & Interfaces*, vol. 34, no. 1, pp. 48-59.

Ramanauskaite, S., Olifer, D., Goranin, N. & Cenys, A. 2013, "Security Ontology for Adaptive Mapping of Security Standards", *International Journal of Computers Communications & Control*, vol. 8, no. 6, pp. 878-890.

Siponen, M. 2006, "Information security standards focus on the existence of process, not its content", *Communications of the ACM*, vol. 49, no. 8, pp. 97-100.

Siponen, M. & Willison, R. 2009, "Information security management standards: Problems and solutions", *Information & Management*, vol. 46, no. 5, pp. 267-270.

Yeniman Yildirim, E., Akalp, G., Aytac, S. & Bayram, N. 2011, "Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey", *International Journal of Information Management*, vol. 31, no. 4, pp. 360-365.

7. Appendix

7.1 Total number of connections

ISO 27002:2005 and KATAKRI comparison summary (c) Riku Nykänen, 2013-2014 Total number of connections.	Administrative security	Personnel security	Physical Security	Information Assurance	
ISO 27001	8	0	0	0	8
4. Risk assessment and treatment	12	0	0	0	12
5. Security policy	21	0	0	0	21
6. Organization of information security	50	5	0	1	56
7 Asset management	11	1	0	7	19
8 Human resources security	20	14	1	1	36
9 Physical and environmental security	0	2	31	20	53
10 Communications and operations management	9	2	1	52	64
11 Access control	0	1	16	73	90
12 Information systems acquisition, development and maintenance	6	0	0	31	37
13 Information security incident management	17	0	0	1	18
14 Business continuity management	15	0	0	8	23
15 Compliance	5	0	0	10	15
Total	174	25	49	204	452

III

TAILORABLE REPRESENTATION OF SECURITY CONTROL CATALOG ON SEMANTIC WIKI

by

Riku Nykänen & Tommi Kärkkäinen 2018

Cyber Security: Power and Technology, 163-177

Reproduced with kind permission of Springer, Cham.

Tailorable Representation of Security Control Catalog on Semantic Wiki

Riku Nykänen and Tommi Kärkkäinen

***Abstract** Selection of security controls to be implemented is an essential part of information security management process in an organization. There exists a number of readily available information security management system standards including control catalogs that could be tailored by the organizations to meet their security objectives. Still, it has been noted that many organizations tend to lack even the implementation of the fundamental security controls. At the same time, semantic wikis have become popular collaboration and information sharing platforms that have proven their strength as an effective way to distribute domain-specific information within an organization. This paper evaluates adequacy of the semantic wiki as security control catalogue platform to build the information security knowledge base that would help especially small and medium sized enterprises to develop and maintain their security baseline.*

Riku Nykänen, Tommi Kärkkäinen
University of Jyväskylä
Jyväskylä, Finland
Email: riku.t.nykanen@student.jyu.fi

Introduction

Taking care of information and cyber security is a must for modern organizations to guarantee the business continuity. Especially small and medium enterprises (SME) struggle with the limited resources and lack of knowledge (Yeniman Yildirim et al. 2011). Information security management system (ISMS) is a commonly applied approach to develop, validate and maintain information security in organizations. Availability of information security management systems that would have been designed to cope with the SMEs is still scarce (Barlette & Fomin, 2008; Lyubimov et al. 2011).

The major information security management systems, including ISO/IEC 27001 (2013) and NIST SP 800-39 (2011), are based on a risk management approach. Hence, organizations perform risk analysis to determine the threats on their assets. In addition to detecting the threats, risk analysis should also reveal the likelihood and impact of the threats to the assets, which are used to prioritize the risks. Based on the prioritization, organization shall implement security controls to mitigate risks or eventually accept the residual risk.

Security control is a countermeasure that mitigates risks caused by the threats. Depending on the characteristics of the organization, different security controls can be beneficial. There exists a number of security control catalogues, including ISO/IEC 27002 (2013), NIST SP 800-53 (2013) and BSI IT Grundschrift Catalog (BSI, 2013), that organizations can use to determine appropriate security controls to meet the organizational security objectives. Security control catalogues are usually presented in the document format, where NIST SP 800-53 makes an exception because it is also available in the structured XML format.

In this article, we propose to establish a tailorable security control catalogue using a semantic wiki. The main research question is to evaluate whether semantic wiki provides a usable platform to construct an organizational knowledge base for information security. Such a knowledge base could provide a platform for SME organizations to reuse and utilize existing public security control catalogues as a service. The contents of the rest of the article are as follows: the next chapter represents necessary background on security controls and semantic wikis. The second chapter states the main research objective and describes the steps of the research process. In the third chapter, results of the research are displayed. The last chapter includes the discussion and ideas for the future work.

Background

Security controls

Some ISMS standards, like ISO 27001 (2013), define the security baseline that sets minimum objectives that the ISMS of the organization shall meet. Organization shall then select security controls that are appropriate for the organizations functions and assets that will mitigate risks to the acceptable level. Fenz et al. (2014) point out that successful control selection is one of the top challenges in the information security management.

There exists a number of approaches to security control selection. For example, widely applied and established ISO/IEC 27001 (2013) defines that organization

shall determine all necessary controls from any source and compare them to comprehensive list of controls defined by the ISO/IEC 27001 Annex A so that no necessary controls are omitted. On the other hand, German BSI IT-Grundschutz Catalogues (BSI, 2013) defines an exhaustive list containing over 1400 security controls where organization can select appropriate controls. For an SME, this is an overwhelming task.

NIST Special Publication 800-53 revision 4 (2013) defines security and privacy controls for federal information systems and organizations. Although this is a specification for federal organizations, it is applicable for enterprises as well (Ross, 2007). The actual control catalogue defines three baselines that could be used; low-impact, moderate-impact and high-impact information systems.

In addition to the baselines, NIST SP 800-53 (2013) defines priority for controls to help an organization to sequence the control implementation. Priority is also defined in the three level scales: P1 (first), P2 (next) and P3 (the last). The specification highlights that priority should not be applied to the control selection, but only in the implementation order of the controls. The security controls that don't belong into any baseline use priority P0.

Because of its structure and availability, NIST SP 800-53 release 4 (2013) was selected as the information security management specification baseline to be used here. The controls of the specification have been published in the XML format. The XML presentation of NIST SP 800-53¹ is an available document containing security controls in the structured format. Other security baseline documents or their control catalogues, like ISO/IEC 27001 (2013) and ISO/IEC 27002 (2013), are not freely available in such a structured format.

Semantic wiki

A wiki is a website that allows one to create, modify and share hypertext content (Lahoud et al. 2014). Wiki systems are becoming more popular knowledge and information management tools. As pointed out by (Kleiner et al. 2009) “wikis are often used as internal collaboration tools in companies or projects in order to facilitate knowledge management between coworkers.” Semantic wikis extend basic wiki platforms with the ability to represent, query and manage structured information. Here our focus is on structured information security knowledge management of the security controls.

In a non-semantic wiki, pages are classified using categories. This means that each page can belong to zero or more categories, which can be used to create

¹ <https://nvd.nist.gov/static/feeds/xml/sp80053/rev4/800-53-controls.xml>

hierarchies of pages. Categories are not usable to perform searches with conditions, but only to classify pages. Hence, semantic wiki can implement more functions dynamically based on the semantic search, which is not possible in the non-semantic wiki platforms.

Semantic wiki adds possibility to define properties that are set on the page. This means, for example, that for each page describing a city, we can include the information on the number of inhabitants. With semantic query it is then possible to search cities with more than 100.000 inhabitants as the queries support comparison operators for semantic properties. With the non-semantic wiki, it is only possible to find pages by classification (categories) or matching text. The semantic search is one of the emphasized functions of semantic wikis and it has been utilized, e.g., by Lahoud et al. (2014), Kleiner et al. (2009) and Garcia et al. (2010), as part of the work to be described next.

Semantic wikis can and have been used in organizations to improve their general knowledge management. Lahoud et al. (2014) propose a dedicated knowledge management system based on a semantic wiki to integrate the views of different business actors in product design projects. A semantic framework for managing IT systems monitoring information, the configuration items, on hosts, services, and network devices was described in Kleiner et al. (2009). In software engineering, a semantic platform to store best practices related to initiation and closing phases of software projects was presented in Elkaffas and Wagih (2013). Garcia et al. (2010) advanced the quality management of software projects by developing an externally audited tool (according to ISO9001:2008) for the quality management system of the project documents. This work is closest to the present work, focusing on the security management. Moreover, Khanom et al. (2015) used the Semantic MediaWiki to construct their demonstrator for the empirical evaluation of their icon-based requirements management approach. A dated summary of possible scenarios is provided by Geisser et al. (2008). To conclude, especially software engineering, systems management, and knowledge base needs have been addressed using semantic wikis, but, as far as we are aware of, this is the first work that proposes to utilize them in the field of information security management.

Technically Semantic MediaWiki (SMW) is an extension to MediaWiki, the platform used by the Wikipedia. It adds semantic annotations to MediaWiki platform that can be used, for example, to organize, tag and search wiki's content (SMW website). SMW will be used here as the basic wiki technology. Note that the same enlarged platform was also used by Elkaffas and Wagih (2013) and García et al (2010).

Construction of security control knowledge base

We propose to transform and manage the security controls of the NIST SP 800-53 specification appendix F on a semantic wiki. Using features of the semantic wiki, we add new viewpoints to the specification to help an organization (especially SME) in selection of the security controls. These views are not available as such in the document format specification or NIST National Vulnerability Database website 800-53 catalogue. (<https://web.nvd.nist.gov/view/800-53/home>)

To be more specific, we utilize the search functions to create dynamic views of the controls where organization can sort and filter controls by the baseline and the priority. In addition, we'll modify the control views to display wider information of the related controls to help an organization in the assessment and selection of the relevant controls.

The realized research and development process was composed of the following steps:

1. Analysis of the NIST SP 800-53 structural model.
2. Mapping of the model to semantic wiki concepts.
3. Building transformations to create structured documents from NIST SP 800-53 contents that was imported into wiki.
4. Validation of the semantic model and the transformation results.
5. Definition of additional views to data using semantic wiki features.

The presented process follows the method for semantic knowledge base construction as presented by Yao et al. (2014). However, the method by Yao et al. (2014) was extended with the additional last step to define new views to the security control catalogue in order to validate the usability of the SMW as the security control knowledge base.

Structural model

Our first step was to analyze the basic structure of the NIST SP 800-53 specification. Analysis was made based on the XML representation of NIST SP 800-53 revision 4 controls. The structural model of the security controls is presented in Figure 1 using UML.

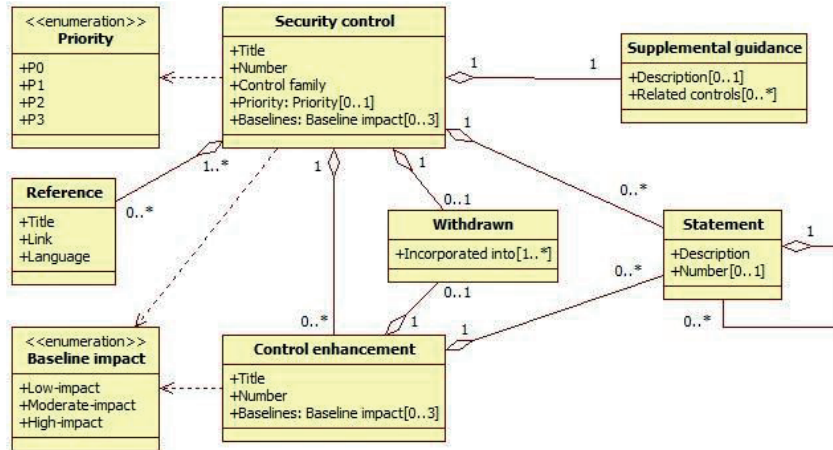


Fig 1. NIST SP 800-53 structural model.

At the highest level of the specification, security controls are grouped into 18 control families. Control families themselves don't have any other property than their title, but they have identifier consisting of two letters. In the XML schema, each security control contains the control family in textual format without any specific datatype for the family.

Security control is identified by a hierarchical identifier, which is the unique for each control. It contains abbreviation of the control family together with the number of the control that is unique within the control family. Each control belongs to only one control family. The security control has a name, defined in the attribute title. Actual description of the control is within the statement, which can contain sub-statements. The most of the controls have also the supplemental guidance that can provide additional implementation considerations or explanatory text (NIST SP 800-53, 2013).

Security controls are divided into three baselines; low, moderate and high impact. A security control can belong to one or more baselines, but some of the compensating controls might not belong to any baseline. The organization shall select pursued baseline based on, first, "strength of security functionality"; and, second, "degree of confidence supported by the depth and coverage of associated security evidence, that the security functionality is complete, consistent, and correct". Where low baseline contains controls that are essential for all organizations, high baseline sets minimum assurance in cases where high security is required. The controls within baselines are not definitive and *the baselines can be tailored to suit the organizational requirements*. In the beginning of the

tailoring process, it is expected that all controls of the selected baseline are implemented, but during the tailoring process some controls may be eliminated or replaced with the compensating controls. (NIST SP 800-53, 2013)

The priority code is attached to each security control, which is meant to help organizations to control the implementation order of the controls. Security controls with priority code 1 are intended to be implemented first, controls with priority code 2 should be implemented next and controls with the priority code 3 at the last. Priority code 0 implies that the security control is not selected in any baseline. Priority codes are intended to be used only to define the implementation order of securing the available resources of the organization, not as the control selection criteria. (NIST SP 800-53, 2013)

Some security controls have one or more control enhancements, which provide additions to the main control. Control enhancements have separate baseline definition and, hence, all enhancements may not be applicable on the same security baseline where base security control belongs to. For example, security control “AC-2 Account management” belongs to baseline low, moderate, and high, but some of its enhancements belong to moderate and high baseline or only to the high baseline. Like security controls, control enhancements are described within the statements, which can contain sub-statements.

The security controls can also have references to other specifications, like other NIST special publications, and external information sources. The references have name and URL properties.

Control catalog ontology for SMW

Gruber (2009) states that “ontology defines a set of representational primitives with which to model a domain of knowledge or discourse”. Primitive concepts in the definition of an ontology are classes, properties (also called attributes) and relations between the classes. The ontology models knowledge of a topic area using the presented primitives.

Table 1 represents the ontology of the security control catalogue for the semantic wiki. It contains four classes that are extracted from the NIST SP 800-53 specification, properties for the classes and relationships between classes. Relationships are presented through property references.

Table 1. Ontology of the security control catalog for semantic wiki.

Class	Property	Type	Constraints	Refers to
Control family	Name	Page		

Security control	Name	Page			
	Identifier	Text			
	Priority	Text	Allowed values P0, P1, P2 and P3.		
	Baselines	Text array	Allowed values Low, Mod and High.		
	Family	Text		Control family - Name	
	Sortkey	Text	2)		
	Description	Text			
	Guidance	Text			
	Related controls	Text array		Security control - Identifier	
	External references	Text array		External reference - Name	
	Retired	Text			
	Incorporated	Text array		1)	
	Control enhancement	Name	Page		
		Identifier	Text		
Baselines		Text array	Allowed values Low, Mod and High.		
Control reference		Text		Security control - Name	
Sortkey		Text	2)		
Description		Text			
Guidance		Text			
Related controls		Text array		Security control - Identifier	
Retired		Text			
Incorporated		Text array		1)	
External reference	Name	Page			
	Link	URL			

- 1) Array elements can refer to a security control or a control enhancement identifier, but there can be also other text.
- 2) Unique string format key based on the control identifier that is generated in the transform. It is used to maintain the logical ordering, when searching wiki pages.

In the definition of the ontology, the data model of the Semantic MediaWiki was taken into account. In the SMW, data is organized to wiki pages having a number of properties. In the SMW, wiki page is identified by the name. From wiki user

point of view, it does not make sense to define pages with the single sentence textual content. Therefore, in the ontology, we combine statements, which are just short textual definitions, into single textual property called 'Description' instead of creating a separate wiki page for each statement. Utilizing this approach, we are able to produce wiki pages that include similar representation of security controls and control enhancements than the document format specification.

In the SMW information is organized into pages. Like in the non-semantic wiki, pages can belong to categories, which are used to group similar pages. Categories match to classes of the definition of the ontology by Gruber (2009), when category is used to group all pages having certain content like a movie, a book or an actor. In a non-semantic wiki, page is usually defined as formatted free text and search operations try to find certain text from the page. In the semantic wiki, each page can define a set of properties that describe contents of the page. As semantic wiki has properties, semantic queries can be implemented to find the pages containing certain values for the properties. Where non-semantic wiki can be search only using free-text search and categories, semantic wikis have more elaborated search options to find the specific content and avoid the problems of free-text search.

In the SMW, it is possible to aggregate information from multiple pages using the semantic search. In the definition of the security control catalog, we utilized this feature on multiple pages to provide more information for a user than just a link to another page. For example, in the listing of controls in a certain control family, we included also identifier, name, priority and baselines of the control. The list is generated automatically based on the set properties in the pages defining the security controls.

MediaWiki has the page template feature, which defines a reusable structure that can be shared by multiple pages. In the Semantic MediaWiki (SMW), it is possible to use semantic properties within such templates. To utilize the defined ontology, we created four templates for the SMW that match the defined ontology classes: Control family, Security control, Control enhancement and External reference. Properties of the classes as presented in Table 1 were directly applied to each page template. The actual wiki pages, which are instances of the classes, are composed from the given properties.

Construction and validation of the transformation

Semantic MediaWiki Data Transfer extension provides XML import functionality. With the extension, it is possible to create wiki pages from the contents of the XML file using the page templates. Hence, we implemented XSL transformations to generate the wiki pages from the NIST SP 800-53 XML file. Table 2 summarizes implemented transformations including their input and output.

Table 2. Implemented XSL transformations.

Transformation	Input data	Output data
Control family	Distinct values of security control elements control family attribute.	Control family element for each distinct value with name attribute defined.
Security control	Security control definition excluding control enhancements.	Security control element with statements aggregated to description property.
Control enhancement	Control enhancements of the each security control.	Control enhancement element with statements aggregated to description property.
References	Distinct values of reference items of security controls.	External reference elements with name and link.

Transformed pages use only properties to define the pages. In other words, pages don't contain any free wiki text, but the page structure is defined in the page templates and the displayed content is set in the properties of each page or generated by the queries, which is explained later.

In the transformation, in addition to properties, name of the page is defined. In the specification there exists few naming conflicts between control families, security controls and control enhancements. For example, "Risk Assessment" is name of the control family and security control RA-3. Because wiki pages must have unique names, identifier of the security control and control enhancement was added to page title to make titles unique.

Validation of the constructed semantic model was performed in two ways. First, we used the SMW build-in special pages. The special pages provide metadata of the SMW contents such as list of all pages, pages with a property, and list of properties. Contents of the special pages were then validated against the original XML file content using XPath expressions to search same data from the XML file. Secondly, validation was also performed using semantic searches, more specifically, using the so-called ask function of the SMW. Again, results of the semantic queries were successfully compared to the results of the XPath statements performed to the original XML file.

Advantages of semantic wiki in construction


To take advantage of semantic wiki functions, we implemented additional views to the security control data that cannot be obtained in the document or the NIST


website format. These functionalities allow especially SMEs to better manage their tailoring process of the security controls.

Listing security controls by priority and baseline

NIST SP 800-53 specification or the NIST website don't provide functionality where one could select a baseline and then order the controls based on their priority. With the semantic wiki such functionality can be implemented using the query form. Form, as shown in Figure 2, is used to input the selected baseline and priority. If either selection is left empty, all values of the property are returned. Selecting the baseline "Low" returns only security controls for the low impact systems and the controls can be ordered in the result table by the shown attribute, like priority.

Run query: Control listing

Baseline :

Priority :

Controls belonging to Low baseline and having P3 priority:





Identifier 	Name 	Baselines 	Priority 
AC-14	Permitted actions without identification or authentication	Low,Mod,High	P3
AC-22	Publicly accessible content	Low,Mod,High	P3
AT-4	Security training records	Low,Mod,High	P3
AU-11	Audit record retention	Low,Mod,High	P3
CA-5	Plan of action and milestones	Low,Mod,High	P3
PE-8	Visitor access records	Low,Mod,High	P3
PS-6	Access agreements	Low,Mod,High	P3
PS-8	Personnel sanctions	Low,Mod,High	P3

Fig 2. SMW page to query security controls by baseline and priority. Both query selections and the resulting table shown.

Listing is generated using the semantic search by finding all pages belonging to the 'Security control' category, having defined values for the properties 'baseline' and 'priority'. If an organization would adopt priorities for its own operations, then search results would be different after the changes of these properties.

List of related controls

In the document format of the NIST SP 800-53, the related controls are listed by their identifiers (number). In the web version, the related controls are still

presented with the identifiers, but also as hyperlinks that can be followed to find out the controls name and other properties. With the controls having multiple related controls, finding their details requires browsing through all the linked pages.

Related controls

Identifier ↕	Name ↕	Priority ↕	Baselines ↕
AC-3	Access enforcement	P1	Low,Mod,High
AC-6	Least privilege	P1	Mod,High
PS-2	Position risk designation	P1	Low,Mod,High
PE-3	Physical access control	P1	Low,Mod,High
PE-4	Access control for transmission medium	P1	Mod,High

Fig 3. Screenshot of the related controls of security control “Separation of duties”.

As shown in Figure 3, we enhanced the view of the security controls by listing the related controls in the table. In the table, we display not only the identifier of the related control but also the name, priority and baseline information. This will help an organization, for example, to choose to implement some low impact controls as they can immediately see what of the related controls are valid on the low-impact baseline. The list is implemented using semantic query as the semantic property of related controls of a security control can be used to execute such a query dynamically.

Control catalog metrics

Semantic search enables to implement various metrics of the control catalog. Figure 4 presents number of different types of pages in the control catalog.

Control catalog metrics

Control metrics	
Number of security controls	256
Number of retired security controls	16
Number of non-retired security controls	240
Control enhancement metrics	
Number of security control enhancements	666
Number of retired security control enhancements	80
Number of non-retired security control enhancements	586
Other metrics	
Control families	18
Number of distinct external references	60

Fig. 4. Control catalog metrics after initial data import from NIST XML source.

Metrics are not limited to the counts of the types of the pages or properties. With SMW template query, it is possible to implement subqueries and provide more complex metrics.

Identifier ↕	Name	Priority ↕	Referring ↕	Referred ▼
AC-3	Access enforcement (AC-3)	P1	19	33
SC-7	Boundary protection (SC-7)	P1	9	24
PM-9	Risk management strategy (PM-9)		1	23
SI-4	Information system monitoring (SI-4)	P1	18	21
CA-7	Continuous monitoring (CA-7)	P2	12	20
AC-2	Account management (AC-2)	P1	21	19
AC-17	Remote access (AC-17)	P1	16	19
CM-6	Configuration settings (CM-6)	P1	5	19
CP-2	Contingency plan (CP-2)	P1	13	19
AC-6	Least privilege (AC-6)	P1	6	17
AT-3	Role-based security training (AT-3)	P1	7	17
MP-4	Media storage (MP-4)	P1	5	16
PE-3	Physical access control (PE-3)	P1	9	16
SA-12	Supply chain protection (SA-12)	P1	17	16

Fig 5. Security controls sorted by number of referrals.

Figure 5 presents referral metrics of the security controls counted using template queries. Template query is required to perform subquery count number of controls referring to each control. In the NIST SP 800-53 (2013), referrals have only one direction. Using semantic template query allows us to calculate for the each

security control the number of other controls it refers to and the number of controls that refers to it, respectively. Hence, the page is result of the execution of multiple wiki page templates. Results can be sorted by any column and in the figure above it is sorted by the “referred” count. We can see from the results that security control “Risk management strategy” refers only to one other control, but is referred by 23 other controls. This can indicate that risk management strategy is a fundamental control that is expected to be implemented by the other controls.

Discussion

In this study, we created the ontology of NIST SP 800-53 (2013) to present the control catalog in the Semantic MediaWiki platform. The created ontology is based on only one specification and, hence, it does not provide universal security control catalog ontology. However, as we have demonstrated, it can be used as basis to create common security knowledge base ontology for SMW based information security knowledge management system. Answer to our main research question is thus positive: *Semantic wiki provides a potential platform to construct an organizational knowledge base for information security.* In our future research, however, we plan to enlarge and augment the elaboration of this question by using SMW as platform to create an extensive security control knowledge base, which would be easy and cost-effective tool especially for small- and medium-sized organizations in their work to ensure security.

The defined ontology can be further enhanced, basically, in two ways. On one hand, it can be extended with additional classes, properties, and relationships from the other NIST Special Publications to create comprehensive NIST Special Publication ontology. On the other hand, it can be generalized to create a generic ontology for security control catalog, which can aggregate the security controls from multiple sources, including other information security management specifications. Hence, the proposed approach provides a basis for knowledge base combining information from multiple security baseline specifications. Such an aggregation, however, requires special context handling, because, for example, “Access control” is a control family in NIST SP 800-53 (2013) specification but the name of the control in ISO/IEC 27001:2013 (2013). Hence we need to introduce some approach to have unambiguous naming in the wiki.

In general, by extending the ontology allows an organization to further benefit from the security control catalog and the support provided for the control selection process (Neubauer et al. 2008). In the implementation of such functionality, semantic search capability is an essential requirement for the control catalog platform. Semantic search functions of semantic wiki platforms provide essential features to advanced management of security control catalogs. We have demonstrated that semantic search can be used in order to create new views on the

contents of the security control catalog, thus helping an organization in its security control selection and tailoring process. This is especially important for SMEs.

Our suggestion here does not mean that an SME would build and maintain the semantic wiki based security control knowledge base, or the established ontology to access the contents, by itself. Instead, by providing such platform as a tailorable service for SMEs that need concrete support to secure their operations can help them to recognize their own possibilities and constraints in information security management. In this work, again, semantic search of the possible controls and their interactions (e.g., metrics) allows SMEs to locate them in the IT security roadmap of given catalogues and measures.

Wiki can also be extended with other properties that would help organization to select appropriate security controls. This would mean that there would be additional properties in the page templates to support additional search criteria. Such attributes could be, for example, work estimates of the implementation of the control that could help organization to select such controls that are applicable with the available resources. This would allow one to elaborate the semantic wiki approach towards a knowledge base that would include also organization and empirical information of the information security controls. This will require extending the defined ontology with other key concepts like threats and assets.

References

- Barlette Y, Fomin VV (2008) Exploring the Suitability of IS Security Management Standards for SMEs. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences, p 308-308.
- BSI (2013) IT-Grundschutz Catalogues. German Federal Office for Information Security (BSI).
- Elkaffas SM, Wagih AS (2013) Use of semantic wiki as a capturing tool for lessons learned in project management. In Proceedings of the Science and Information Conference (SAI), p 727-731.
- Fenz S, Heurix J, Neubauer T et al (2014) Current challenges in information security risk management. *Info Mngmnt & Comp Security* 22(5):410-430. doi:10.1108/IMCS-07-2013-0053.
- García R, Gil R, Gimeno JM et al (2010) Semantic wiki for quality management in software development projects. *Iet Software* 4(6):386-395.
- Geisser M, Happel H, Hildenbrand T et al (2008) New Applications for Wikis in Software Engineering. In: PRIMIMUM.
- Gruber T (2009) Ontology. In: Encyclopedia of Database Systems. Springer US, p 1963-1965.

- ISO/IEC 27001:2013 (2013) Information technology – Security techniques – Information security management systems – Requirements. ISO copyright office. Geneva, Switzerland.
- ISO/IEC 27002:2013 (2013) Information technology – Security techniques – Information security management systems – Code of practice for information security management. ISO/IEC.
- Khanom S, Heimbürger A, Kärkkäinen T (2015) Can icons enhance requirements engineering work?. *Journal of Visual Languages & Computing* 28:147-162. doi:<http://dx.doi.org/10.1016/j.jvlc.2014.12.011>.
- Kleiner F, Abecker A, Brinkmann SF (2009) WiSyMon: Managing Systems Monitoring Information in Semantic Wikis. In *Proceedings of Third International Conference on Advances in Semantic Processing, SEMAPRO '09*, p 77-85.
- Lahoud I, Monticolo D, Hilaire V (2014) A semantic wiki to share and reuse knowledge into extended enterprise. In *Proceedings of Tenth International IEEE Conference on Signal-Image Technology and Internet-Based Systems (SITIS)*, p 702-708.
- Lyubimov A, Cheremushkin D, Andreeva N et al (2011) Information Security Integral Engineering Technique and its Application in ISMS Design. In *Proceedings of Sixth International Conference on Availability, Reliability and Security (ARES)*, p 585-590.
- Neubauer T, Ekelhart A, Fenz S (2008) Interactive Selection of ISO 27001 Controls under Multiple Objectives. In: Jajodia S, Samarati P, Cimato S (eds) *Proceedings of The Ifip Tc 11 23rd International Information Security Conference*, vol 278. Springer US, p 477-492.
- NIST Special Publication 800-39 (2011) *Managing Information Security Risk: Organization, Mission, and Information System View*.
- NIST Special Publication 800-53 Revision 4 (2013) *Security and Privacy Controls for Federal Information Systems and Organizations*.
- Ross R (2007) Managing Enterprise Security Risk with NIST Standards. *Computer* 40(8):88-91. doi:[10.1109/MC.2007.284](http://dx.doi.org/10.1109/MC.2007.284).
- Yeniman Yildirim E, Akalp G, Aytac S et al (2011) Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *Int J Inf Manage* 31(4):360-365. doi:<http://dx.doi.org/10.1016/j.ijinfomgt.2010.10.006>.
- Yuangang Yao, Xiaoyu Ma, Hui Liu et al (2014) A Semantic Knowledge Base Construction Method for Information Security. In *Proceedings of the IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2014 on, p 803-808.

IV

SUPPORTING CYBER RESILIENCE WITH SEMANTIC WIKI

by

Riku Nykänen & Tommi Kärkkäinen 2016

OpenSym '16: Proceedings of the 12th International Symposium on Open
Collaboration, article 21

Reproduced with kind permission of ACM.

Supporting Cyber Resilience with Semantic Wiki

Riku Nykänen
University of Jyväskylä
P.O. Box 35 (Agora)
FIN-40014 University of Jyväskylä, Finland
+358 50 384 3733
riku.t.nykanen@student.jyu.fi

Tommi Kärkkäinen
University of Jyväskylä
P.O. Box 35 (Agora)
FIN-40014 University of Jyväskylä, Finland
+358 40 567 7854
tommi.karkkainen@jyu.fi

ABSTRACT

Cyber resilient organizations, their functions and computing infrastructures, should be tolerant towards rapid and unexpected changes in the environment. Information security is an organization-wide common mission; whose success strongly depends on efficient knowledge sharing. For this purpose, semantic wikis have proved their strength as a flexible collaboration and knowledge sharing platforms. However, there has not been notable academic research on how semantic wikis could be used as information security management platform in organizations for improved cyber resilience. In this paper, we propose to use semantic wiki as an agile information security management platform. More precisely, the wiki contents are based on the structured model of the NIST Special Publication 800-53 information security control catalogue that is extended in the research with the additional properties that support the information security management and especially the security control implementation. We present common uses cases to manage the information security in organizations and how the use cases can be implemented using the semantic wiki platform. As organizations seek cyber resilience, where focus is in the availability of cyber-related assets and services, we extend the control selection with option to focus on availability. The results of the study show that a semantic wiki based information security management and collaboration platform can provide a cost-efficient solution for improved cyber resilience, especially for small and medium sized organizations that struggle to develop information security with the limited resources.

CCS Concepts

• Security and privacy—Systems security, Human and societal aspects of security and privacy

Keywords

Cyber resilience, Risk management; Information security management; Semantic wiki.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.
OpenSym '16, August 17-19, 2016, Berlin, Germany
© 2016 ACM. ISBN 978-1-4503-4451-7/16/08\$15.00
DOI: <http://dx.doi.org/10.1145/2957792.2957803>

1. INTRODUCTION

The free Oxford dictionary defines “resilience” as “the capacity to recover quickly from difficulties; toughness”. Such property has become essential for both organizations and computing systems in Digital Era, because the overall functionality supported by the IT infrastructure should be resilient, i.e., tolerant towards rapid and unexpected changes (shocks, disturbances) in the operative environment [2, 14]. The paradigm of resilience, with multiple perspectives and different conceptualizations, for reliable business management was reviewed in [3], where it was pointed out that resilient business operations should tackle both threats and opportunities of the environment. General resilience taxonomy was proposed in [23], which consisted of four dimensions: i) type of shock or perturbation, ii) target system, iii) type of concern, and iv) type of recovery. As will be shown below, very similar conceptualization underlines information security management processes through recognizing and documenting threats on assets with proper control actions to deal with the risks. Concerning the computing infrastructure, resilience of general self-adaptive software systems was advanced in [6], where the concept of resilience was directly linked to the dependability of software systems by requiring trusted delivery of services when facing changes in the system itself or its execution environment. Two metrics to quantify the contribution of a component to the system’s resilience were derived in [9], in order to advance Critical Infrastructure Protection.

Resilience against information security threats has also become more and more important for all kind of organizations. It has been admitted that constant state of flawless security is unreachable as threat landscape evolves continuously [24]. Risk-aware processes focus on the mitigation of the known risks at the design time, but may fail to ensure continuous business operation in the challenging, unexpected conditions [21]. In any case, to manage the information security, organizations need to recognize all valuable assets, identify threats and risks, respond to risks by appropriate controls, and finally monitor the development [24, 31]. Semantic wikis provide excellent platform and infrastructure for the documentation and maintenance of this valuable information.

Even if all organizations share common threats of modern cyber-age, many organizations still struggle to implement even the fundamental security controls [19]. Without proper documentation, organizations may fail to understand their security baseline, which significantly decreases their cyber resilience. Selection of the most important security controls to mitigate security risks is an essential part of the organizations’ risk management process. There exists a range of quantitative methods that support organizations in their security control selection, but these require existence of detailed numeric input data, like risk realization statistics, life-cycle costs of controls and proper asset valuation, in order to provide valid results [29]. However, for small and medium sized organizations (SMEs)

additional resources are usually required to make the necessary organizational data available and to validate it. Hence, especially for SMEs, there is an obvious need for more agile methods to obtain sufficient cyber resilience against both known and emerging threats.

This paper evaluates possibility to use semantic wiki platform as a basis to manage the necessary knowledge on information security to increase the organizational resilience. We propose to use the semantic wiki to provide a platform of existing common information and cyber security information, which can be used as a technical tool for organizations own risk management processes. The proposal consists of initial asset, risk, and security control data provided in the semantic wiki as well as new functions implemented to wiki for common actions performed as part of risk management process. The evaluation focus on analysis that can semantic wiki platform with presented functions be used to overcome common problems of the information security risk management.

2. BACKGROUND

2.1 Information security risk management

The fact that flawless state of information security is unreachable has been widely accepted by the security experts [24]. The most widely used information security management systems, like ISO/IEC 27001 [18], are therefore risk driven and attempt to reach the best possible level of security with available resources.

There exists number of information security ontologies where some focus on the common concepts, like [4] and [11], and others on the specific subdomains of information security, like cloud computing or incident management [1]. Where more comprehensive ontologies require more expertise, which SMEs usually lack, for our novel approach it is essential to start with a simple core ontology that is easy to comprehend and adopt.

Common Criteria (ISO/IEC 1540) is a product security certification standard, which defines widely accepted common model for the key security concepts. The security concepts and their relations as defined in Common Criteria (CC) are described in Figure 1. The same concepts are also included in more extensive ontologies [4, 11].

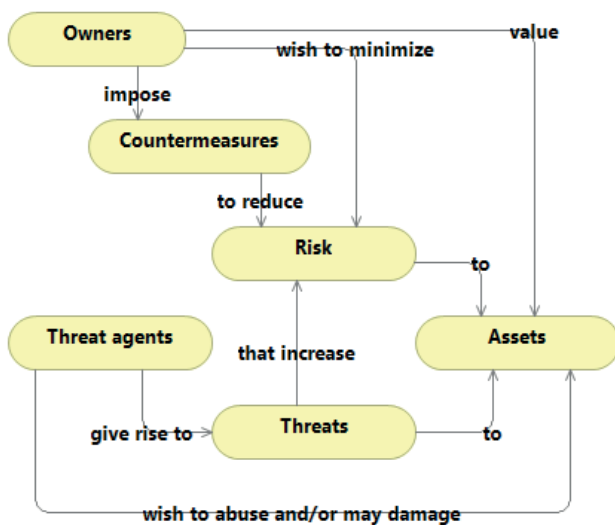


Figure 1 Security concepts and relations by Common Criteria.

In CC, asset is an item, thing or entity that has potential or actual value to an organization (ISO 55000:2014). Control (i.e., countermeasure) is a measure that is modifying risk (ISO/Guide 73:2009). Vulnerability is a weakness of an asset or control that can be exploited by one or more threats (ISO/IEC 27000:2014). Threat is a potential cause of an unwanted incident, which may result in harm to a system or organization (ISO/IEC 27000:2014). Risk is an effect of uncertainty on objectives (ISO/Guide 73:2009). When compared to the resilience taxonomy as proposed in [23] (see Section 1), one can readily identify shocks or perturbations on the target system with threats on assets. Similarly, type of concern and type of recovery in [23] correspond to risks and their countermeasures in CC.

Information security, by the definition, means preservation of confidentiality, integrity and availability (CIA) of information [17]. To preserve all three CIA properties, it is crucial that organizations detect all assets that have an effect to the information security. These are not limited only to physical or information assets, but also organization's processes, culture and other intangible assets should be considered in order to succeed in the asset detection. Information security management system (ISMS) has become the authoritative convention to ensure information security [15]. ISMS defines the organizations security goals, and resources and practices to reach the goals. In addition, it sets how organization monitors and develops its security practices.

Widely used ISO/IEC 27001 ISMS standard applies ISO/IEC 27005 risk management process as part of ISMS implementation [18]. There exists also number of other information security risk management standards and practices like OCTAVE, NIST SP 800-30 and CRAMM. All these share common parts of the risk management process. Table 1 presents typical risk management phases, which have been collected and generalized from multiple specifications by [12].

Table 1. ISRM process phases, tasks and outcomes [12].

Process phase	Typical tasks	Phase outcomes
System characterization	Asset identification	Asset inventory
Threat and vulnerability assessment	Threat and vulnerability identification	List of threats and corresponding vulnerabilities
Risk determination	Likelihood and impact assessment, risk estimation	Risk figures and levels for identified threats
Control identification	Control evaluation	List of recommended controls to mitigate risks
Control evaluation and implementation	Risk treatment; control selection and implementation	List of controls that have reduced risk to acceptable level

Common first task of the risk management process is to know what you have to protect. The knowledge of owned assets, tangible and intangible, are collected to asset inventory. By the definition, asset can be anything that has value for the organization.

The next step in the generalized process by [12] is to identify the vulnerabilities of the assets. Vulnerabilities are accessed by the threats. Hence, we need to identify vulnerabilities and threats that can cause harm to the assets and therefore disrupt organizations operation. As result we should know what to protect (asset

inventory), how it can be harmed (vulnerability inventory), and what can harm it (threat inventory).

After the threat and vulnerability assessment the generalized process by [12] continues with the risk analysis. The risk analysis phase includes assessing threat likelihood and impact of realization of the risk. As the result, we are able to know the risk level and potentially even the damages caused by the realized risks. Risks also can be prioritized by the risk level.

When we are aware which risks have high risk level, the next action is to identify potential controls to mitigate the risks. This is often done using a control catalogue like ISO/IEC 27002 or NIST SP 800-53, which list the common security controls and provide implementation guidance. As the result of control identification, we obtain a list of the potential controls to implement.

The final step of the typical risk management process is to evaluate controls and implement the selected controls. The control selection should take into account already implemented controls, but also costs of the control implementation. Control implementation include development costs (e.g. installation costs), operational costs (e.g. maintenance costs) and response costs (e.g. personnel necessary to operate the countermeasure).

2.2 Challenges of risk management from information security perspective

Comprehensive literature review [13] indicates several challenges in the information security risk management. The encountered common challenges are:

1. To establish asset and control inventory
2. To assign values on assets
3. To predict the risks correctly
4. To avoid overconfidence on the ISMS
5. To share knowledge
6. To balance risk vs. cost trade-offs

The items 1-3 are all related to identification of assets and controls and estimation of values of assets and probabilities of the risks. All these issues are critical for the successful implementation of a quantitative risk analysis method.

Risk analysis methods can generally be divided into two major categories; qualitative and quantitative. Quantitative risk analysis methods rely on derived measures (numbers) to select the best possible risk processing option. Major problem of quantitative methods is lengthy and time-consuming process, which requires detailed information of the asset values and the possible incidents [29]. Qualitative methods are not based on monetary values and mathematics, but merely on the on judgments and perceptions of the evaluated scenario and suitable safeguards for it. Neither of the methods is superior to each other and they are suitable for different kind of organizations [30].

The overconfidence effect is more human problem as we, as humans, tend to assume risk estimates far too optimistic, which biases the outcome of risk, probability, threat and impact assessments. The research [13] also highlights that none of the evaluated eight risk management approaches, including NIST SP 800-30, ISO/IEC 27005, and OCTAVE, does not include any means to overcome the effects of the overconfidence.

Failed knowledge sharing creates a clear deficiency of organizational security and risk management. When independent units of organization, projects and persons share information, their awareness of assets, threats and controls increases, which leads to higher quality of the risk management process. It is noted that knowledge sharing needs motivation and benefits of it must be

mutual. Also [16] highlights the continuous communication and tailored messaging as success factors of the effective risk management.

The last of the listed challenges is the risk vs cost trade-offs. As already discussed, it is hard to provide valid input data, including effectiveness values, weights, dependencies, etc, for the risk analysis. In addition, costs caused by successful attacks are almost impossible to calculate, as they are not limited only to financial loss of the attacked organization, but also indirect collateral damages to customers, partners, and other stakeholders. Successful attack may cause also losses not measurable by money as loss of the personal data or reputation. [5, 13] Trade-offs will exist in the control selection as long as we are not able to provide valid input data and metrics for the specific scenario. Hence, even qualitative risk analysis has its own limitations, it is more suitable for SMEs that lack resources, data and competence to implement the more complex quantitative risk analysis.

2.3 Information security knowledge bases

Knowledge is considered as an important resource for organizations to ensure the continuous business operations. Experience and expertise of the employees will help organization to react in accurate manner to exceptions, when these people understand the complexities of the organization and its operations. Hence knowledge of the employees is having important impact to organizational resilience [27].

Importance of the knowledge sharing as part of the information security risk management has been noted in several researches [13, 16]. Organizational information sharing is an omnichannel activity, including discussions, training, documentation, creation of knowledge bases, etc.

It has been identified in [6, 10] that organizations are not inclined to share information security knowledge in the public web portals as security information is seen as valuable asset against competitors. Although inter-organizational security knowledge sharing has hinders, intra-organizational knowledge sharing with wikis has been proven successful [20, 22]. Knowledge sharing has been noted to require personal trust to other peers and similar incentives. Knowledge sharing and collaboration has also been noted to play an important role in the organizational security risk mitigation [28].

Wiki platforms are becoming more and more popular knowledge and information management tools especial for intra-organizational collaboration to facilitate knowledge management between coworkers [20, 22]. Semantic MediaWiki (SMW) extends basic wiki platforms with the ability to represent, query and manage structured information [22]. Wikis, especially with the semantic extensions, have proven their strengths as knowledge sharing and collaboration platforms for wide variety of purposes especially in software engineering, systems management, and knowledge base systems [26]. Hence, SMW can be seen as a potential collaboration platform for cyber security risk management and associated catalogues for SMEs.

In our previous research [26], we created a novel approach to security control catalogue implementation utilizing the Semantic MediaWiki platform. More precisely, we imported existing NIST SP 800-53 [25] control specification to SMW and created presentations, not available in the document format or NIST SP website, to provide additional viewpoints to security control selection. Additionally, semantic queries were implemented to provide viewpoints to the control catalogue that are not possible with document format specification. As a result, SMW was proven

to provide a potential platform to implement more extensive support for the cyber security risk management.

3. KNOWLEDGE BASE FOR INFORMATION SECURITY RISK MANAGEMENT

3.1 Purpose of research

The main purpose of the current research efforts is to assess, by constructing a prototype, whether it is possible to use semantic wiki as platform for information security knowledge base to improve cyber resilience and risk management processes of especially SMEs. For this purpose, we extend the control catalogue metamodel from our previous research [26] with the risk entity types to enable risk management operations. With the proposed extensions organizations are able to use the knowledge base in two different manners: 1) information source in security control selection, or 2) to implement risk management processes.

Additionally, we evaluate whether, using the proposed approach, it is possible to overcome also other common challenges in the information security risk management presented by [13].

3.2 The construction process

Main phases of the actual realization of the prototype were as follows:

1. Extended SMW metamodel with the risk type taxonomy.
 - a. Define SMW templates.
 - b. Import selected taxonomy.
 - c. Create links from control catalogue to risk taxonomy defining, which risk types each security control mitigates.
2. Extend control catalogue to support resilience driven control selection.
 - a. Add CIA properties to control catalogue and update Security control semantic form.
 - b. Utilize semantic search to support view the controls by CIA properties and existing priorities
3. Provide means to manage risks in the wiki.
 - a. Create semantic forms to add, modify and retire risks.
 - b. Utilize semantic search to browse and review risks.

The construction process was iterative in the sense that semantic search functions for all the main phases we added and modified after more semantic properties became available.

3.3 Implementation

3.3.1 Extended metamodel

At the first phase of the research, we extended the existing control catalogue metamodel to include risk management related ontology definition.

The initial metamodel of the control catalogue was described in [26]. The catalogue was extended with three new types; risk, risk class and CIA. This extended metamodel is presented as UML diagram in Figure 2. CIA is enumeration of the CIA triage including values of confidentiality, integrity and availability. Purpose of the enumeration is to classify the controls based on the CIA property they preserve and hence help organizations to select controls that provide the best support for organizational security goals. Risk class is used to implement the cyber security risk taxonomy to classify controls by the types of the risk they mitigate.

The purpose of the risk class is to help organization to short list controls that are suitable for the identified risk type. As last, the security risk represents an instance of identified, concrete security risk in the organization, such as fire in the “fire in the server room at Abbey Road office”. It is added to the metamodel to support basic risk management functions.

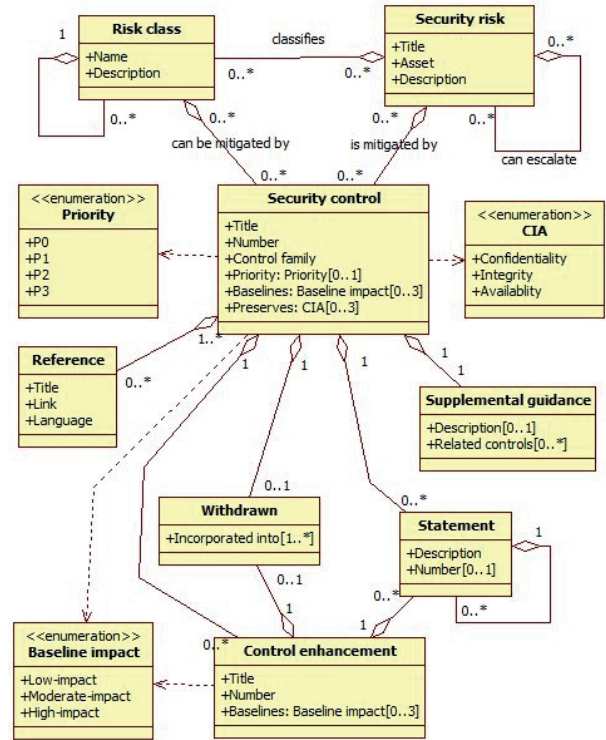


Figure 2: Metamodel UML definition.

3.3.2 Risk taxonomy

In [7] a taxonomy of the operational cyber security risks is defined. The taxonomy has four main classes of the risks.

- actions of people: action, or lack of action, taken by people either deliberately or accidentally, which has impact to cyber security
- systems and technology failures: failures of hardware, software, and information systems
- failed internal processes: problems in the internal business processes that impact the ability to implement, manage, and sustain cyber security, such as process design, execution, and control
- external events: issues originating outside of the organization, such as disasters, legal issues, business issues, and service provider dependencies

Each of the main classes are further divided into multiple subclasses, which are described by their elements. The following list presents subclasses by the main classes.

1. Actions of people
 - 1.1. Inadvertent
 - 1.2. Errors
 - 1.3. Omissions
2. Systems and Technology Failures
 - 2.1. Hardware
 - 2.2. Software
 - 2.3. Systems

- 3. Failed Internal Processes
 - 3.1. Process design and execution
 - 3.2. Process controls
 - 3.3. Supporting processes
- 4. External events
 - 4.1. Disasters
 - 4.2. Legal issues
 - 4.3. Business issues
 - 4.4. Service dependencies

The risks can cascade, which means that a risk in one class can trigger risks in another class. For example, external disaster, like fire, can cause malfunctioning hardware. Due to the cascading effect, it is difficult to predict all actual costs of the realized risks.

The wiki implementation contains taxonomy based on the presented definition by [7]. The HierarchyBuilder extension of SMW can be used to visualize the taxonomy as presented in Figure 3.

Risk classes

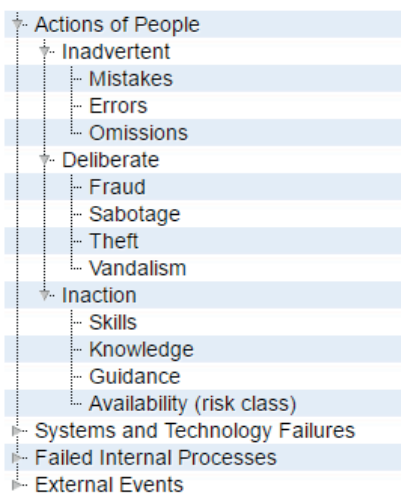


Figure 3 Screen capture of the “Risk classes” wiki page.

Risk class is implemented as page template in the SMW. Instead of separating risk class, subclass and element, we create similar hierarchy using referencing to the parent class. At the prototype implementation, reference is implemented as many-to-one relationship, which means that the risk taxonomy must create a hierarchy. It is possible to later update the relationship to many-to-many enabling also more complex risk taxonomies to be used, if seen necessary.

3.3.3 Control inventory

The control inventory used in the research was based on our previous research [26], where we imported controls of the NIST SP 800-53 [25] specification to SMW. The controls are available by the NIST in XML format and our earlier efforts included XSL transformation of the controls from the NIST defined XML schema to the XML schema used by the SMW page templates.

To help organizations in the control selection based on the aspect of the CIA triage, we added to the NIST SP 800-53 control catalogue metadata which identifies what triage attributes the corresponding control supports. Each control can support one or more of the confidentiality, integrity and availability properties. As described earlier, the organizational resilience is mostly driven by

the availability and less dependent on the integrity and confidentiality. This does not mean that integrity and confidentiality should be disregarded, but provides merely one viewpoint to support the control selection by the SMEs. For example, omitting privacy as part of confidentiality can lead to realization of the legal risks and lead to severe sanctions.

Availability

Availability is one of the three main properties defining the information security among confidentiality and integrity. ISO/IEC 27000 defines that confidentiality is a property of being accessible and usable upon demand by an authorized entity.

Controls ensuring availability [edit]

Control family [+]

Baselines [-]

High Low Mod

Priority [-]

P0 P1 P2

Mitigates [+]

Control	Control family	Baselines	Priority	Mitigates
Security awareness and training policy and procedures (AT-1)	Awareness and training	Low Mod High	P1	Training and development Actions of People Notifications and alerts Escalation of issues
Security awareness training (AT-2)	Awareness and training	Low Mod High	P1	Actions of People Training and development Notifications and alerts Escalation of issues

Figure 4 Screen capture of controls preserving availability.

The practicability of the SMW and its extension can be seen in Figure 4, where semantic search is associated to Semantic Result Formats extension enabling to filter the controls. NIST SP 800-53 contains 240 active controls and 586 active control enhancements, which makes effective search and filtering capabilities essential. In the figure, the controls ensuring availability are listed and filters limit the display to only controls on low baseline (controls that should be implemented always) and priority level 1 (highest priority controls to implement). With this query and semantic filtering, we are able to display the highest priority controls to implement to maintain the availability. From the cyber security risk management point of view, these are precisely the controls that are critical to support organizational resilience.

Training and development

Description [edit]

Failure to maintain the appropriate skills within the workforce.

Mitigating controls [edit]

Control family [+]

Baselines [-]

High Low Mod

Priority [-]

P1 P2 P3

CIA properties [-]

Availability Confidentiality Integrity

Mitigates [+]

Name	Control family	Baselines	Priority	CIA properties	Mitigates
Security awareness and training policy and procedures (AT-1)	Awareness and training	Low Mod High	P1	Confidentiality Integrity Availability	Training and development Actions of People Notifications and alerts Escalation of issues
Security awareness training (AT-2)	Awareness and training	Low Mod High	P1	Confidentiality Integrity Availability	Actions of People Training and development Notifications and alerts Escalation of issues

Figure 5 Training and development risk class.

For the risk class template, we created a query that displays the controls that are applicable to mitigate risks of the class. As risk classes are defined in the three levels and each control is attached to a risk class on any level, it is necessary to implement query to find all subclasses of the defined risk class. So instead of searching only the class, we use array of class and its subclasses as the search

criteria. The search is performed to find all controls that have one or more of the items in the mitigation property array. As result, the table of controls mitigating the risk class is displayed on the page of the each risk class as shown in Figure 5 Training and development risk class. To help organizations to select and prioritize the controls, a filter functionality is applied to the search results. Hence, user can select, for example, priority P1 and low baseline security controls, which are the ones expected to be implemented first for all information systems including the ones having even low impact and requiring only the fundamental security controls to be implemented.

3.3.4 Risk management functions

The risk analysis includes evaluation of the risk probability and its impact. One of the most used methods for the risk analysis are the risk matrices. The risk matrix contains two axes; likelihood and impact. The risk matrix is used to identify the high likelihood and high impact risks and decrease either or both the likelihood and the impact to mitigate the risk. However, risk matrices are criticized of not providing sufficient support for good decision making and being limited to only subjective risk evaluation. [8]

Instead of using the risk matrix type of risk analysis, we propose to use queries to identify the risks that need attention. As risks cascade there is a relationship between the risks. Hence, we include in the risk definition an attribute that gives us possibility to define unidirectional cascading relationship between any two risks. With additional queries, we are able to rank the risks by using the cascading measures. For example, if a risk refers to many other risks that will be realized due to realization of the risk, then this is an indication of importance of that particular risk and should be taken into account in the risk analysis and control selection. In the qualitative risk analysis such information can be used to predict risk more accurately and decrease the overconfidence effect.

Create Security risk: Hardware failure of a workstation

Figure 6 Form to add new security risk.

To allow organizations to manage their own risks with the SMW instance, a security risk template was added. For simplified risk management solution it contains only a limited number of attributes. Each risk has name, description, textual description of

assets and risk classes it belongs. Additionally, there are controls that have been implemented to mitigate the risk and list of other risks that can cascade from realization this risk. The security risk form was created to input the risks. The form is presented in Figure 6 Form to add new security risk.

Security risk template is used to review a risk. In addition to displaying user entered information, the template lists security controls that mitigate risk classes defined for the risk, but which are not implemented. Result of such a query is displayed to the user as a list of potential controls. Figure 7 provides screen capture of a sample listing.

Fire in office server room

Fire in office server room

Contents [hide]	Classes Fire
1 Description	Implemented controls
2 Assets	
3 Cascading risks	
4 Potential controls	

Description [edit]

Fire in the office server room cause hardware failures to servers and network devices in the server room. Also all the services provided by the devices in the server room can fail.

Assets [edit]

Servers, information in system X

Cascading risks [edit]

Backups are destroyed, Domain controller hardware failure, Office network gateway failure

Potential controls [edit]

	Control family	CIA properties
Media storage (MP-4)	Media protection	Availability Confidentiality
Fire protection (PE-13)	Physical and environmental protection	Availability
Alternate work site (PE-17)	Physical and environmental protection	Availability

Figure 7 Sample risk instance screen capture.

These functions allow organization to use the SMW as a basic risk management platform to identify the risks by using the cyber security risk taxonomy, and perform qualitative risk analysis to evaluate the potential security controls to mitigate the risks. With addition of the CIA properties, the organization is able to filter the set of potential controls to focus on resilience, especially from the availability point of view. Although the resilience is more than implementation of the security controls preserving availability, implemented knowledge base will help users to overcome the lack of knowledge of controls and their effect to cyber resilience of the organization.

4. EVALUATION

4.1 Unique naming requirement

As noted in our earlier research [26], one of the difficulties with the implementation is the unique naming requirement of the wiki pages. Mainly this causes problems with the extensions, like HierarchyBuilder, that use the explicit page names instead of defined properties in the visualization. Example of the problem can be seen in Figure 4, where Availability has disambiguation to refer to the risk class instead of the page Availability, which contains

information of the CIA triage property availability and lists all controls preserving availability.

4.2 Response to risk management challenges

In addition to realizing the prototype we analyzed how the MediaWiki based platform responds to the information security risk management challenges as defined in [13] (see Section 2.2). The first challenge was asset and countermeasure inventory, where the response is partial. The extended control inventory provides the countermeasure, but structured asset inventory is not currently included. This is a notable deficiency in the prototype and should be fixed in the further development. Lack of the asset inventory is also causing lack of support of the second challenge of assigning asset values.

The third challenge by [13] is failed predictions of risks. This challenge is partially solved by the support to identify cascading risk and, hence, having better knowledge of the risk realization probability. Note, though, that because the metamodel does not currently support statistic of the risks or risk types, such an evaluation is a subjective one. This could be solved by extending the metamodel with the statistics and more detailed information of the realized risks and occurred incidents. The problem remains, if no public statistics are available or if statistics are not accurate.

The fourth and fifth challenge by [13] are overconfidence effect and knowledge sharing. With the organizational wiki, we are able to overcome the problem of knowledge sharing at least from the platform point of view. Still the organizational culture must support the knowledge sharing of the cyber security risks and the security controls. The overconfidence effect lead too optimistic risk estimates [13]. This can be at least reduced with the increased knowledge of the related risks and available controls.

Risk vs cost trade-offs is the last challenge by [13]. The prototype is not currently able to respond to this challenge as the risk analysis uses qualitative approach instead of supporting quantitative information. As noted by in [13], solution would require detailed risk management approach, which is not seen suitable for SMEs because of the necessary resource allocation needed.

Overall it can be seen that the prototype partially solves problems, especially with knowledge sharing, and the proposed approach increases the overall understanding of the risks and their relationships. Lack of asset inventory can be seen as deficiency that should be analyzed in detail and solved in further development, but technical limitations from SMW point of view do not limit such extension.

4.3 Improved cyber resilience

Cyber resilience and ensuring cyber asset and service availability has become critical topic, when number of cyber threats is increasing and protection from the all threats is financially unfeasible. To support availability aspect, we introduced traditional information security CIA properties to control catalogue to help the controls selection from availability point of view.

In the NIST SP 800-53 control catalogue there is 115 low impact level controls and 87 of those are on priority level 1. These are the controls that are expected to be implemented in all information systems at the first phase. If we wish to focus on the resilience and the controls especially supporting availability, we can reduce the number of these first phase controls in our classification to about 50 controls.

Limitation of the usage of the CIA properties is that many controls support all three properties, but have direct impact on one property. Example of such control is AC-3 Access Enforcement. Primarily it

supports confidentiality, but it has also impact on the availability. Although, we are able to provide support for cyber resilience using the CIA properties, extended classification should be introduced in the future.

4.4 Limitations of the research

Current metamodel does not include asset inventory and support asset-driven approach to security control selection. More comprehensive security risk management taxonomies are readily available [27]. In order to help organizations in the identification of the assets, use of such a taxonomy should be realized.

5. DISCUSSION

Our proposed semantic wiki based approach to manage information security risk knowledge within the organizations provides a technical platform for organizations to start controlled cyber security risk management. While the proposed platform has publicly available information as prefilled contents, it provides, especially for SMEs lacking extensive cyber security skills, easier way to exclude the irrelevant risks and controls rather than inventing appropriate controls with limited knowledge.

SMW has proven to be a valid platform to share the structured information within the organizations. Where people are used to user interface familiar from Wikipedia, there is a low barrier to start using such a system in the collaboration. With the semantic search functions, we are able to find the risks that have high cascading effect to availability, the most import CIA property from the resilience point of view.

Although current implementation provides basic functionalities for the risk analysis, the current metamodel has its limitations. Current model of the wiki is based on the NIST SP 800-53 control catalog. The catalogue is not complete set of security controls, although it is comprehensive. To create an extensive information security knowledge base, we need to create a true ontology for semantic wiki that harmonizes concepts from the main data sources.

Assets and countermeasures are ontologically connected through vulnerabilities and threats. Vulnerabilities exist in the assets and are used by the treats where countermeasures mitigate the threats. These concepts are excluded from the metamodel as it is not seen essential for the SME point of view to maintain threat and vulnerability catalogues. Although it is information that has meaning for the risk analysis, it should be further considered whether there would be centralized repository for threats and vulnerabilities, which can be replicated to organization specific wiki instances. Also asset and risk taxonomies could include centralized management.

Metamodel excludes elements of the incident management, which would be essential for a continuous risk management process. When incident information would be available in the wiki, it could be linked to assets or asset types and also to risks. This would enable an organization to monitor effectiveness of the implemented controls and provides statistical information for the quantitative risk analysis.

Our research continues with extending and generalizing the metamodel to be able to provide more extensive platform for SMEs to manage their information and cyber security risks. The future research focuses to develop cyber risk management platform for SMEs based on the SMW, which has proven its strengths as a platform for security knowledge bases.

6. REFERENCES

- [1] Arbanas, K. and Čubrilo, M. Ontology in Information Security. *Journal of Information and Organizational Sciences*, 39, 2 (2015).
- [2] Bhamra, R., Dani, S. and Burnard, K. Resilience: the concept, a literature review and future directions. *Int J Prod Res*, 49, 18 (09/15 2011), 5375-5393.
- [3] Birkie, S. E., Trucco, P. and Kaulio, M. State-of-the-Art Review on Operational Resilience: Concept, Scope and Gaps. (2013), 273-280. DOI=10.1007/978-3-642-40361-3_35.
- [4] Blanco, C., Lasheras, J., Fernández-Medina, E., Valencia-García, R. and Toval, A. Basis for an integrated security ontology according to a systematic review of existing proposals. *Computer Standards & Interfaces*, 33, 4 (6 2011), 372-388. DOI=10.1016/j.csi.2010.12.002.
- [5] Caldwell, T. The true cost of being hacked. *Computer Fraud & Security*, 2014, 6 (6 2014), 8-13. DOI=http://dx.doi.org/10.1016/S1361-3723(14)70500-7.
- [6] Camara, J., de Lemos, R., Laranjeiro, N., Ventura, R. and Vieira, M. Robustness-Driven Resilience Evaluation of Self-Adaptive Software Systems. *IEEE Transactions on Dependable and Secure Computing*, PP, 99 (2015), 1-1.
- [7] Cebula, J. J., Popeck, M. and Young, L. A Taxonomy of Operational Cyber Security Risks Version 2. (2014).
- [8] Cox, L. A. What's Wrong with Risk Matrices? *Risk Analysis*, 28, 2 (2008), 497-512.
- [9] Fang, Y. P., Pedroni, N. and Zio, E. Resilience-Based Component Importance Measures for Critical Infrastructure Network Systems. *IEEE Transactions on Reliability*, PP, 99 (2016), 1-11. DOI=10.1109/TR.2016.2521761.
- [10] Feledi, D. and Fenz, S. Challenges of Web-Based Information Security Knowledge Sharing. *Proceedings of the Seventh International Conference on Availability, Reliability and Security (ARES)*, 2012, 514-521.
- [11] Fenz, S. and Ekelhart, A. Formalizing information security knowledge. In *Anonymous Proceedings of the 4th international Symposium on information, Computer, and Communications Security*. ACM, 2009, 183-194.
- [12] Fenz, S. and Ekelhart, A. Verification, Validation, and Evaluation in Information Security Risk Management. *Security & Privacy*, IEEE, 9, 2 (2011), 58-65.
- [13] Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. Current challenges in information security risk management. *Info Mngmnt & Comp Security*, 22, 5 (11/10; 2015/12 2014), 410-430. DOI=10.1108/IMCS-07-2013-0053.
- [14] Hilton, J., Wright, C. and Kiparoglou, V. Building resilience into systems. In *Anonymous Systems Conference (SysCon)*, 2012 IEEE International, 2012, 1-8.
- [15] Humphreys, E. Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, 13, 4 (11 2008), 247-255.
- [16] Hunt, R. Why governance, risk and compliance projects fail – and how to prevent it. *Computer Fraud & Security*, 2014, 6 (6 2014), 5-7.
- [17] ISO/IEC 27000:2014. Information technology — Security techniques — Information security management systems — Overview and vocabulary. ISO copyright office, Geneva, Switzerland, 2014.
- [18] ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. ISO copyright office, Geneva, Switzerland, 2013.
- [19] Julisch, K. Understanding and overcoming cyber security anti-patterns. *Computer Networks*, 57, 10 (7/5 2013), 2206-2211. DOI=http://dx.doi.org/10.1016/j.comnet.2012.11.023.
- [20] Kleiner, F., Abecker, A. and Brinkmann, S. F. WiSyMon: Managing Systems Monitoring Information in Semantic Wikis. *Third International Conference on Advances in Semantic Processing*, 2009. SEMAPRO '09, 2009, 77-85.
- [21] Koslowski, T. and Zimmermann, C. Towards a Detective Approach to Process-Centered Resilience. In *Proceedings of the Security and Trust Management: 9th International Workshop, STM 2013*, Egham, UK, September 12-13, 2013. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013, 176-190.
- [22] Lahoud, I., Monticolo, D. and Hilaire, V. A semantic wiki to share and reuse knowledge into extended enterprise. In *Tenth International Conference on Signal-Image Technology and Internet-Based Systems (SITIS)*, 2014. IEEE, 2014, 702-708.
- [23] Maruyama, H., Legaspi, R., Minami, K. and Yamagata, Y. General resilience: Taxonomy and strategies. *International Conference and Utility Exhibition on Green Energy for Sustainable Development (ICUE)*, 2014, 1-8.
- [24] Müller, G., Koslowski, T. G. and Accorsi, R. Resilience-A New Research Field in Business Information Systems? *Business Information Systems Workshops*. Springer, 2013, 3-14.
- [25] NIST Special Publication 800-53 Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology, 2013.
- [26] Nykänen, R. and Kärkkäinen, T. Tailorable Representation of Security Control Catalog on Semantic Wiki. Submitted, 2016.
- [27] P. Shamala and R. Ahmad. A proposed taxonomy of assets for information security risk assessment (ISRA). *Fourth World Congress on Information and Communication Technologies (WICT)*, 2014, 29-33.
- [28] Safa, N. S., Solms, R. v. and Fitcher, L. Human aspects of information security in organisations. *Computer Fraud & Security*, 2016, 2 (2 2016), 15-18.
- [29] Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. Taxonomy of information security risk assessment (ISRA). *Computers & Security*. 57 (3 2016), 14-30.
- [30] Tatar, Ü. and Karabacak, B. An hierarchical asset valuation method for information security risk analysis. In *Anonymous Information Society (i-Society)*, 2012 International Conference on. (.), 2012, 286-291.
- [31] Zahoransky, R. M., Brenig, C. and Koslowski, T. Towards a Process-Centered Resilience Framework. *2015 10th International Conference on Availability, Reliability and Security (ARES)*, 2015, 266-273.

V

**A KNOWLEDGE INTERFACE SYSTEM FOR INFORMATION
AND CYBER SECURITY USING SEMANTIC WIKI**

by

Riku Nykänen & Tommi Kärkkäinen 2018

Designing for a Digital and Globalized World, DESRIST 2018, 316-330

Reproduced with kind permission of Springer, Cham.

A knowledge interface system for information and cyber security using semantic wiki

Riku Nykänen and Tommi Kärkkäinen

University of Jyväskylä, Finland

Abstract. Resilience against information and cyber security threats has become an essential ability for organizations to maintain business continuity. As bullet-proof security is an unattainable goal, organizations need to concentrate to select optimal countermeasures against information and cyber security threats. Implementation of cyber risk management actions require special knowledge and resources, which especially small and medium-size enterprises often lack. Information and cyber security risk management establish knowledge intensive business processes, which can be assisted with a proper knowledge management system. This paper analyzes how Semantic MediaWiki could be used as a platform to assist organizations, especially small and medium-sized enterprises, in their information and cyber security risk management. The approach adopts design science research and service design methodologies in the derivation and evaluation of the system.

Keywords: Information Security, Cyber Security, Design Science Research, Knowledge Management, Risk Management.

1 Introduction

In the recent decade, the importance of information security (IS) has constantly increased for all businesses. Proper management of IS provides competitive advantage, whereas shortcomings can constitute a serious source of risks. Hence, risk management activities are needed in all sized organizations, but small and medium-size enterprises (SMEs) are still struggling to manage their information security and implement basic security controls [33]. Information security management standards do exist, but the focus of the standards is the existence of policies and processes, and not how they can be accomplished in practice [38]. It has been also noted that existing standards do not take into account the special needs of SMEs [45].

Information security risk management is faced with multiple challenges, especially related to assets, security-cost trade-offs, and cost estimation in general [10]. Security knowledge management emphasizes the asset protection [32]. The asset availability, i.e., proper identification and organization of the competencies, processes, and technological resources for IS, was found to have the largest indirect effect on the organization performance [14].

Humans still provide the most significant risks related to information security [11]. Information security policies and procedures have an important role for SMEs, who with limited resources typically just focus on keeping the necessary technology up and

running in their everyday security management [4]. However, the technological choices might not be the most effective ones [13]. Even two thirds of the risk reducing controls in SMEs might not be designed properly or not operating as expected, mostly due to underestimating the risk level [34]. To conclude, especially SMEs need support in their IS risk management in order to select cost-effective countermeasures against increasing cyber and information security threats.

Information security management system (ISMS) has become common practice to define organizations' information security management goals and practices. ISO/IEC 27001 [18] is a widely adopted international standard, which defines requirements for ISMS and specifies security controls that an organization needs to implement. The controls are described in detail in the ISO/IEC 27002 standard [19]. There exist also other control catalogues, like NIST SP 800-53 [27] and BSI IT Grundschutz Catalogues [5]. All the three mentioned ISMS specifications establish risk-driven approach. ISO/IEC 27001 has been extended to support cyber security domain with the descriptive standard ISO/IEC 27032 [20].

In the cyber domain, risk management activities are similar to information security risk management (ISRM). One must identify assets; assess vulnerabilities and threats; evaluate risk; and select appropriate controls and implement them [9]. Where information security protects information assets, cyber security focuses protecting assets reachable via cyberspace [44]. As information is in the modern organizations stored in digital form, it is also reachable via cyberspace. Hence, information security and cyber security overlap, but there are also physical assets, which can be compromised via cyberspace, for example, devices that can be controlled and monitored using SCADA systems. Hence, it is more and more vital for SMEs to establish proper security risk management procedures to understand and mitigate both information and cyber security risks.

In the information security context, risk evaluation and control selection methodologies can be divided into three categories; quantitative, qualitative, and hybrid (semi-quantitative) [37]. In the quantitative methods, one derives a numeric estimate of the risk realization probability and cost and then selects optimal controls to mitigate the risk based on the return of the investment. Qualitative methods, on the other hand, are more knowledge-driven and the control selection is based on expertise of the stakeholders [37]. Hence, risk management processes are knowledge-driven, so they can be referred as knowledge intensive business processes (KIBP). Availability of expertise and knowledge is essential.

Our objective is to use design science research in developing an information and cyber security knowledge management artifact that provides operational support for organizations in the information and cyber risk management. To lower the adaptation barrier, the artifact should respond to the existing challenges of especially SMEs. These challenges include availability of resources, like money and knowledge. Hence, the artifact should especially tackle the knowledge gap of SMEs not utilizing the existing information and cyber security baselines to support their risk management activities. The solution should also be scalable and variable for different types of the organizations to avoid limiting the users of the artifact to a specific business domain or size. The

artifact development encompasses an ongoing research activity, where all design science research cycles have been executed at least once. Here, the role of KIBP in relation to the rigor cycle [15, 16], as an existing knowledge-intensive process, is emphasized. It is taken into account in the design cycle, by utilizing challenges of KIBP as identified in [26] in the evaluation framework of the artifact.

2 Background

2.1 Information and cyber security risk management

There exists a number of reference models for information security risk management. Fenz & Ekelhart [9] have identified the common information security risk management phases from widely adopted models: *i) System characterization*: identification of the scope of the risk management activities; *ii) Threat and vulnerability assessment*: identification of possible scenarios how a risk could be realized; *iii) Risk determination*: evaluation of the probability of the risk and impact of the realized risk; *iv) Control identification*: identification of possible countermeasures to mitigate the risks; *v) Control evaluation and implementation*: selection and implementation of the controls that mitigate a risk to an acceptable level.

As a process, organization shall, after setting the scope of the risk management activities, identify the assets that are needed in the operations. Asset is, by the definition, something that has value for the organization [18]. For the risk assessment, organization identifies possible threats targeting the assets. The risk determination focuses on the evaluation of the likelihood and impact of the risks, which also includes valuation of the assets for the organization. Also other properties can be evaluated to prioritize risks. The control evaluation aims to select optimal controls to mitigate the one or more of the risks. In the control evaluation, there are four ways to address a particular risk: *i) Accept*: Organization understands the risk and its consequences, but decides not to address it in other manner; *ii) Avoid*: Activities exposing organization to a risk are avoided; *iii) Transfer*: Consequences of the realized risk are transferred to other party; *iv) Mitigate*: Countermeasures are implemented to reduce the risk to an acceptable level.

In general, the risk management may fail in all phases [9]. Fenz et al. [10] highlights that common failures are asset identification and valuation, risk prediction and control selection. Especially asset valuation and risk prediction are critical phases for quantitative methods. The quantitative methods require detailed information of the asset values and incident likelihood [37]. Qualitative approach relies on judgments and perceptions of the evaluated scenario and proposes suitable safeguards for it [40]. This highlights the need for knowledge management and sharing. Although, neither of the methods is superior to other, qualitative methods are less time consuming [40] and hence can be, in general, more suitable for SMEs with limited resources.

Although, users are often noted as the “weakest link” of the chain of security, they also have valuable information for security risk management process [39]. Collaboration can be also seen as one factor to engage employees to security and its enhancement.

Vice versa, lack of knowledge sharing is one of the common challenges of the information security risk management [9]. Knowledge sharing also increases security awareness, which has direct impact on organizations capability to protect themselves against cyber-attacks [23]. Therefore, knowledge management, and knowledge management systems, hold an essential role in information and cyber security risk management processes.

2.2 On Knowledge-Intensive Business Services and Processes

The continuous increase of knowledge intensity in the digital economy was recognized in [1] and the importance of knowledge in information security risk management was pointed out in [7]. Knowledge-Intensive Business Services (KIBS) refer to a versatile set of both professional and technology-based services, which are characterized by high demands of professional knowledge and relevant information sources as the key ingredients of service design [24]. As usual, one separates the explicit and tacit knowledge. Note that in [1] it is noticed that KIBS are often developed and innovated by SMEs. KIBS are utilized in knowledge-intensive business processes (KIBP).

Belsis et al. [3] point out that security management of information systems is a knowledge-intensive activity that depends on professional knowledge. They also argue that the knowledge dimension of the security management, e.g., transformation of raw log or survey data into actionable knowledge, has been neglected. Hence, security management support requires KIBS. This is mostly addressed by the systems school of knowledge management whose primary focus is on information and knowledge-based systems [7], especially structure and usefulness of databases, repositories, and platforms containing codified and accessible explicit knowledge about the domain of interest [6].

A complex decision making is often not solved by a single user, but it is solved by the collaborative contributions of multiple participants [2]. Conduct and execution of knowledge-intensive business processes heavily dependent on knowledge workers performing various interconnected knowledge intensive decision making tasks [41]. As genuinely knowledge, information and data centric processes, IS risk management process meets definition of KIBP. Characteristics of knowledge-intensive business processes compared non-KIBP [17] are presented in Table 1.

Table 1. KIBP compared non-KIBP [17].

KIBP	Non-KIBP
Mostly complex	Simple or complex
Mostly hard to automate	Mostly easy to automate
Mostly repeatable	Highly repeatable
Predictable or unpredictable	Highly Predictable
Need lots of creativity	Need less creativity
Structured or semi/unstructured	Structured

The challenges of information and cyber security risk management in [7, 10] emphasize the presence of KIBP characteristics compared to the non-KIBP characteristics. Mundbrod & Reichert [26] represent eight challenges of Knowledge-Intensive Business Processes:

- *Meta-model design*: design of the meta-model that supports required information and tasks.
- *Lifecycle support*: KIBPs require both design and runtime flexibility, which applies also tools used in the conduction of the processes.
- *Variability support*: KIBP results heavily depend on the knowledge used on the process, which requires high variability.
- *Context Support*: related to lifecycle and variability support, KIBPs can be very specific for certain context, which requires support for contextual parameters.
- *View support*: when amount of activities and knowledge required in processes conduction and execution is high, requirement for personal views emerges.
- *Authorization support*: KIBP execution includes variety of tasks and information, which include collaboration of people in various roles, authorization support is necessity from security perspective.
- *Synchronization support*: successful task execution requires that all the necessary information is available on the time. Therefore, synchronization of the information and documentation is required.
- *Integration support*: KIBP may directly correlate and initiate pre-specified and standardized business processes. Hence, integration is required to receive status updates and get outputs of the processes.

The presented KIBP challenges apply also to information and cyber security risk management and we adopt these challenges in the evaluation of the presented artifact.

2.3 Knowledge Management Systems

Knowledge management systems are utilized in KIBP to support the execution of the complex processes [17]. From risk management perspective, knowledge is considered as an important resource for organizations to ensure the business continuity. Experience and expertise of the employees will help organization to react in accurate manner when incidents occur as people understand the complexities of the organization and its operations. Knowledge sharing is also a necessity in information security risk management [10].

Wiki platforms are popular knowledge and information management tools especial for intra-organizational collaboration, and have been applied in variety of business processes [28]. Semantic additions, like Semantic MediaWiki (SMW), provide opportunity to define and manage structured information in the wiki platforms, which are by nature usually non-structured. Semantic wiki adds possibility to define properties for each wiki page. This means, for example, that for each page describing a city, the number of inhabitants can be defined. With semantic query, it is then possible to search cities with more than 100.000 inhabitants as the queries support comparison operators for semantic

properties. With the non-semantic wiki, it is only possible to find pages by classification (categories) or matching text. The semantic search is one of the emphasized functions of semantic wikis and enables complex functions implemented with the wiki platform.

There is difference between managing security knowledge and securing knowledge management. Jennex & Zyngier [21] discusses aspects how to secure knowledge management and related processes, while this paper focuses on management of security information. Anyway, it is important to consider the security of the information security knowledge management system and its service delivery to avoid lack of confidence to system's security as an adaptation barrier.

3 Research process

The research follows the Design Science Research (DSR) approach, which includes development of a set of artifacts to solve a wicked problem [15]. DSR is composed of the three related cycles: i) the relevance cycle, ii) the rigor cycle, and iii) the design cycle. The relevance cycle ensures that technology-based solutions solve important and relevant business problems. The rigor cycle provides the prior scientific knowledge and theories as a foundation to the research [15, 16], but also ensures that rigorous methods are applied in the construction and evaluation of the design artifact [43]. The design cycle contributes as the construction and evaluation phase of the artifact. Note that Peffers et al. [30] presented more refined composition of DSR steps as follows: i) identify problem, ii) define solution objectives; iii) design and development, iv) demonstration, v) evaluation, and vi) communication.

Based on the DSR approach, the goal of this research is to develop and evaluate an artifact, the demonstrator consisting of multiple components, that provides a solution to information and cyber security risk management challenges of, especially, SME organizations. We apply the criteria defined by Venable [42] to assess DSR applicability for the research.

An overview of the methodologies for designing services is proposed by Morelli [25]. He advises one of the three main directions "definition of possible service scenarios, verifying use cases, and sequences of actions and actors' roles in order to define the requirements for the service and its logical and organizational structure". Also, Edvardsson [8] includes service system as part of the service design in addition to service concept and service processes. The service system includes resources and infrastructure enabling delivery of the service.

4 Artifact description

4.1 Artifact development

Development of a software system is newer confined to the successive steps [35]. Although we adopt an existing software platform, the development of the information security knowledge management system is a combination of software development and data migration. The development iterations follow the identified information and cyber

security risk management use cases. During each development iteration, the meta-model for information security controls is extended as new wiki functions are introduced. The changes of the meta-model also affect to the import of the knowledge information from public data sources.

Hence, we apply iterative design process in the construction of the artifact, which is described in Figure 1. The iterative approach also corresponds to DSR cycles, although there are multiple development cycles for a one design and evaluation DSR cycle. The relevance cycle is focused on identifying the problems within the information and cyber security risk management of the SMEs. Also common practices are evaluated and why SMEs fail to implement them. In the rigor cycle, the main developed asset is the meta-model, which is the basis for the system's demonstrator. The design cycle implements the actual functions on top of the SMW platform utilizing the meta-model. Also the evaluation of demonstrator is part of the design cycle.

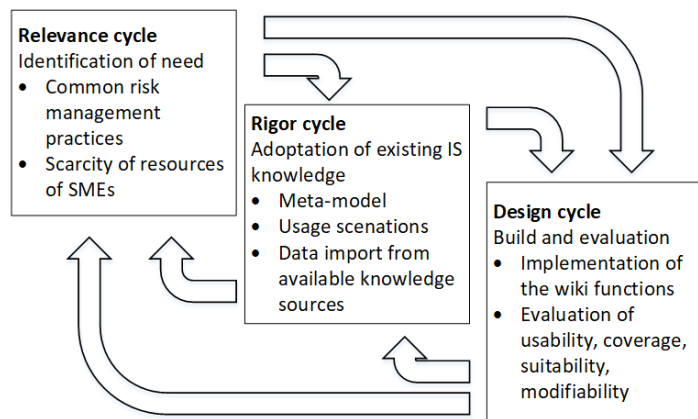


Fig. 1. Iterative design process presenting DSR cycles with outcomes of the cycles.

Iterative development is applied to three main artifacts that are developed in parallel; meta-model, data import and wiki functions. The meta-model is in the central position as both, data import and wiki functions depend on it. The meta-model will evolve during the development iterations as new functions are being introduced. Hence, the two iterative development loops both affect the meta-model as shown in Figure 2. This is similar approach as the concept of reciprocal shaping of ADR presented in [36], where recursive cycles of decisions at finer levels of detail of the IT artifact and the organizational context.

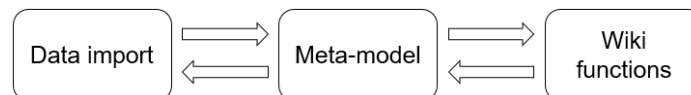


Fig. 2. Development cycles of the demonstrator.

In the development process, the wiki functions refer to the additional risk management functionality implemented and added to the SMW platform. These functions are derived from the common risk management process tasks, which are part of the common

risk management approaches. Such functions are, for example, asset identification, risk evaluation, and control selection. For example, if user recognizes assets of a certain type, the wiki queries can be used to propose security controls that mitigate risks for the asset type and in addition these control implementation order can be prioritized based on the priorities defined in NIST SP 800-53 specification. Common use cases are identified following the service design principles. Each use case adds new incrementally new functionality to demonstrator following the activities of demonstration and evaluation by Peffers et al. [30]. The main required functions (see Sections 1-2) are asset identification, threat identification, risk evaluation, control identification, and control evaluation.

As a result of the asset identification, an organization should have recognized and valued at least all the business critical assets. Valuation of the assets is important as all assets don't have similar importance for the organization. Assets valuation is usually performed with numeric value in quantitative methods or with classification of assets in qualitative methods [37].

Treat identification can be assisted using a threat catalogue. ISO 27002 [19] or NIST SP 800-53 [27] include only control catalogues, but BSI IT Grundschatz Catalogues [5] includes also a threat catalogue in addition to control catalogue. The user should be assisted to identify the threats, for example, by the asset types an organization is having. This requires that threats are classified by the asset types. In this process, knowledge of the assets within the organization is a mandatory requirement to perform successful identification.

In the risk evaluation, the organization shall perform estimation on how a realized risk may be handled. The common four ways to address the risk are accepting, avoiding, transferring, or mitigating a particular risk (see Section 2.1). Regardless of the handling method, the organization should document the actions and explanation for the decision. The documentation of the rationale will increase knowledge sharing compared to the tacit knowledge of undocumented decisions.

Control identification can be helped with the control catalogue [5, 19, 27]. When controls are linked to threats they are preventing, the threat identification also generates a list of potential controls. The organization shall select and document control implementation status of the selected countermeasures. Based on the risk assessment, organization shall have a list of the prioritized list of controls to be implemented. The prioritization is based on the priorities of security controls defined in NIST SP 800-53 baseline. In the SMW platform queries are defined to provide views to list i) controls that are implemented, ii) controls that are selected to be implemented, but implementation is not completed and iii) controls that are for the time being excluded.

4.2 Artifact components

The research aims to create a knowledge-based system that helps especially SME organizations in their cyber risk management activities. As SMEs struggle with limited resources for cyber security risk management, at the same time there exists variety of publicly available information in multiple knowledge bases. Bringing this data with the

viewpoints that adapt to organization's needs, is expected to help the organizations to manage their cyber risks.

The developed artifact consists of the following components:

- Model of security concepts relevant for SMEs to create a security knowledge base
- Demonstrator of the information and cyber security risk management system
- Data-gathering templates

We adopt the roles of Knowledge Interface Systems (KIS) by Gregor et al. [12] in the following diagram.

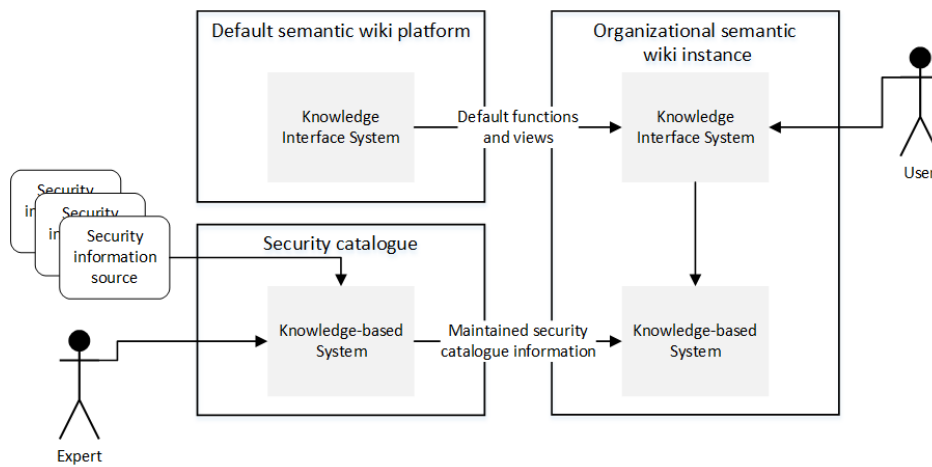


Fig. 3. Role of knowledge interface system and knowledge base.

The system shall use information and cyber security knowledge from public sources like NIST SP 800-53 control catalogue [27] as well as other control catalogues [5, 19, 20]. Each of the utilized control catalogues is mapped to the meta-model, which is developed as part of the system. Hence, organizations shall have publicly available information ready in the knowledge-based system.

The common knowledge base updates are delivered by the service, which will also maintain the platform itself. However, the SMW platform enables organizations to add new functions also by themselves utilizing new templates and queries, if the supported use cases don't include all functions required by the organization. As an individual organization operates with the separate wiki instance, the modifications are not disseminated to other organizations.

The knowledge itself is not a solution to successfully accomplish cyber risk management activities. Therefore, knowledge platform needs to be extended with the functions to enable to perform cyber risk management activities. The SMW enables adding template pages and use queries to evolve knowledge base to a system that implements functions of a risk management system. SMW also enables to extend the meta-model based on the organization's needs, unlike many other risk management tools. We have

developed [28] a meta-model for security control catalogue with risk management functions. The meta-model has evolved from security control catalogue meta-model to contain also risk management elements. Further development iterations are required to support all the use cases identified in the rigor cycle.

4.3 Description of the demonstrator

Demonstrator is based on the Semantic MediaWiki (SMW) platform. MediaWiki is a software mostly known by its use as the software platform of the Wikipedia. The SMW is an extension to MediaWiki, which enables semantic functions to be used. Such functions are structured pages and semantic queries.

Advantage of the MediaWiki is that users are familiar with the basic functions of the platform. The SMW enables using MediaWiki as a knowledge management platform [28]. With the forms, users can enter also new data, like assets and risk evaluations, in the structured form. In addition to the structured data, the traditional wikitext descriptions can also be used. Such semi-structured approach enables better variability for different purposes compared to a fixed data-model. More detailed description of the control catalogue and the basic risk management functions have been given in [28].

SMW Data Transfer plugin is used to import existing security controls specification data into SMW platform. In the first iteration, NIST SP 800-53 control specification [27], which is available in XML format, was transformed using XSLT to XML schema defined by the developed meta-model. After the transformation, Data Transfer plugin generates wiki-page for each control at the import.

Demonstrator is delivered for user organizations as own wiki instances. Each instance will be delivered as a service, but could also be set up by the organization as own in-premises instance of the wiki, if seen feasible, for example, for the security reasons. The deliverable consists of the SMW platform, added functionality and templates as well as imported data. When an organization takes the service into use, it shall define users and apply roles. After that, the organization can start performing cyber and risk management activities with the system.

5 Evaluation

5.1 Research evaluation

Evaluation of the research is performed following the evaluation criteria for assessing DSR work defined by Venable [42]:

- Relevance of the problem to industry/society clearly established
- Significance of the problem to industry/society clearly established
- Depth of analysis and clarity of understanding of the problem and its causes
- Depth or profoundness of insight leading to the new design artefact
- Novelty of the new design artefact
- Size and complexity of the new design artefact
- Amount of effort that went into the development of the new design artefact(s)

- Elegance of the design of the new artefact(s)
- Simplicity of the design of the new artefact(s)
- Clear understanding of why the new artefact works

The significance and “wickedness” of the problem has been identified in the number of the papers and reports [13, 14, 22, 45]. Also the causes of the problem have been identified in those papers, which consistently highlight the lack of resources and suitable methods and tools.

The profoundness of the artifact has been identified by following the common risk management process activities as identified by Fenz et al. [9]. The developed artifact must respond to activities in each phase of the process with appropriate manner.

The artifact approaches the information security risk management problem from knowledge management perspective. The wiki-based knowledge management systems have been utilized in multiple domains, as identified in [31], but in the domain of the information security there does not exist similar artifacts.

The design of the artifact aims to be simple as it reuses existing knowledge management platform, SMW, and extends its functionality. The simple approach provides users a familiar interface, but also the meta-model defining the data structure is modifiable, if organization has special needs or requirements. With this approach, the adaptation barrier should remain low as the artifact can respond to competence, usability and modifiability requirements.

The service delivery of the artifact has also been covered in the artifact design as proposed by [8]. The service delivery is especially important aspect in this research as SMEs don’t have resources to take into use complex systems, only to support decision making. This is the weakness of SMW platform as it is intended to be used for knowledge sharing. Therefore, it lacks support to have multiple knowledge bases within one instance of platform. Although MediaWiki provides concept of namespaces, it does not sufficient functionality to separate confidential information of multiple organizations within one instance. There are multiple options to solve the lifecycle challenge as deployment of new instance could be automated using container technologies. As this is more technical issue, it is left outside of the scope of the research.

5.2 Response to KIBP challenges

Table 2 contains responses to the challenges of KIBP identified in [26] as presented in Section 2.2.

Table 2. Response to KIBP challenges.

Challenge	Response
Meta-model design	Meta-model is an integral part of the developed artifact. It is utilized by the KIS when security information from the public knowledge bases is mapped to the meta-model.
Lifecycle and variability support	SMW, as a platform, enables modification of the functions without platform modifications. Lifecycle and variability support shall be also considered in the meta-model. Deployment of the

	platform as a service can be considered as a weakness of the solution. Each user organization must have a separate instance of the SMW platform.
Context support	Context support shall be considered in the meta-model, but can be also implemented as part of SMW page definitions.
View support	View support can be implemented with the semantic queries and extendibility of the SMW platform. The platform enables users to create pages that meet the personal needs.
Authorization Support	SMW platform has built-in authorization functions. The built-in functions may be extended to meet more complex authorization scheme requirements.
Synchronization and integration support	SMW platform has possibility to integrate other data sources as well as build functional integrations. Synchronization support must be taken into account in the meta-model design.

As can be seen from the responses, the meta-model and SMW platform with additional functions are in essential position to overcome these common challenges. To avoid the challenges, the iterative research and development cycles are applied. The most weakest response to KIBP challenges is with the lifecycle support, which is already covered in the evaluation of the service delivery.

5.3 Validation using data-gathering templates

Survey-based empirical evaluation among SMEs shall be performed utilizing data-gathering templates. The evaluation shall include survey of SME users of the artifact. Survey should request response to following topics, which are seen to be advantage of the artefact.

- Did the artifact improve the resource usage and competence requirements in SMEs?
- Were the proposed functions comprehensive for organization's needs?
- Is a risk management system using SMW user interface easy to adopt in a SME context?
- Was organization able to find suitable security controls to implement based on the suggestions made by the platform?
- Did the organizations modify the SMW meta-model or wiki functions? If yes, what kind of modifications an organization made? The latter question should evaluate completeness of the artifact.

Other survey topics can be introduced, when identified during the DSR development cycle. Results of the evaluation shall be communicated as design science methods suggest.

6 Conclusions

Importance of information and cyber security risk management has become a necessity for all-sized organizations. Especially SMEs have not implemented all the required security measures to protect themselves. Often the reason for this is the lack of competence and other resources required to implement proper risk management processes.

This paper represented a research process adopting design science research to develop and evaluate novel knowledge based approach for information and cyber security risk management. The developed artifact is based on the SMW platform, which is extended with the additional functionality for risk management and incorporated with the information security information available in public specifications.

The research is currently in progress. In the initial cycle, as described in [29], the initial meta-model with control inventory was implemented including import of the NIST SP 800-53 control inventory. During the next cycle, we extended the meta-model to support features critical for cyber resilience as well as basic risk management features in [28]. In the future, the artifact is enhanced with the meta-model and risk management functions supporting the common risk management process phases supporting all phases from asset identification to control implementation.

The research process involves characteristics of Action Design Research (ADR) [36], where the ongoing nature of the development of the semantic wiki based artifact has been depicted in the earlier publications [28, 29]. Moreover, the research problem arises from the information and cyber security practices of SMEs, incorporating both knowledge and risk management theories. Also, following the ADR principles, the research is practice inspired seeking solution to problems of information and cyber security risk management from intersection of IT and risk management domains.

Design science research provides an appropriate framework to identify relevant foundations of the artifact as well as to develop and evaluate the artifact, being both practice-inspired and theory-ingrained [36]. As described, there is practical need for a system assisting SMEs in their information and cyber risk management activities. We have argued the potential of the knowledge-based approach to meet these needs.

References

1. Bahrs J., Müller C. (2005) Modelling and Analysis of Knowledge Intensive Business Processes. In: Althoff K, Dengel A, Bergmann R et al (eds) Professional Knowledge Management: Third Biennial Conference, WM 2005, Kaiserslautern, Germany, April 10-13, 2005, Revised Selected Papers Springer Berlin Heidelberg, Berlin, Heidelberg, p 243-247.
2. Baumeister J., Striffler A. (2015) Knowledge-driven systems for episodic decision support. *Knowledge-Based Syst* 88:45-56.
3. Belsis P., Kokolakis S., Kiountouzis E. (2005) Information systems security from a knowledge management perspective. *Information Management & Computer Security* 13(3):189-202.
4. Bhattacharya D. (2011) Leadership styles and information security in small businesses. *Information Management & Computer Security* 19(5):300-312.

5. Bundesamt für Sicherheit in der Informationstechnik (2015) IT-Grundschutz Catalogues, 15th edn.
6. Cox L.A., Babayev D., Huber W. (2005) Some Limitations of Qualitative Risk Rating Systems. *Risk Analysis* 25(3):651-662.
7. dos Santos França J.B., Netto J.M., Barradas R.G., Santoro F., Baião F.A. (2013) Towards Knowledge-Intensive Processes Representation. In: La Rosa M., Soffer P. (eds) *Business Process Management Workshops: BPM 2012 International Workshops*, Tallinn, Estonia, September 3, 2012. Revised Papers Springer Berlin Heidelberg, Berlin, Heidelberg.
8. Edvardsson B. (1997) Quality in new service development: Key concepts and a frame of reference. *International Journal of Production Economics* 52(1):31-46.
9. Fenz S., Ekelhart A. (2011) Verification, Validation, and Evaluation in Information Security Risk Management. *Security & Privacy, IEEE* 9(2):58-65.
10. Fenz S., Heurix J., Neubauer T., Pechstein, F. (2014) Current challenges in information security risk management. *Info Mngmnt & Comp Security* 22(5):410-430.
11. Furnell S.M., Clarke N., Komatsu, A., Takagi, D., Takemura, T. (2013) Human aspects of information security: An empirical study of intentional versus actual behavior. *Information Management & Computer Security* 21(1):5-15.
12. Gregor S., Maedche A., Morana S., Schacht, S. (2016) Designing knowledge interface systems: Past, present, and future. In: *Breakthroughs and Emerging Insights from Ongoing Design Science Projects: Research-in-progress papers and poster presentations from the 11th International Conference on Design Science Research in Information Systems and Technology (DESRIST) 2016*.
13. Gupta A., Hammond R. (2005) Information systems security issues and decisions for small businesses: An empirical examination. *Information management & computer security* 13(4).
14. Hall J.H., Sarkani S., Mazzuchi T.A. (2011) Impacts of organizational capabilities in information security. *Information Management & Computer Security* 19(3):155-176.
15. Hevner, A.R. (2007) A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems* 19(2):87-92.
16. Iivari, J. (2007) A Paradigmatic Analysis of Information Systems As a Design Science. *Scandinavian Journal of Information Systems* 19(2): 39-64,
17. Işık Ö., Mertens W., Van den Bergh J. (2013) Practices of knowledge intensive process management: Quantitative insights. *Business Process Management Journal* 19(3):515-534.
18. ISO/IEC 27001:2013 (2013) Information technology – Security techniques – Information security management systems – Requirements. ISO copyright office. Geneva, Switzerland.
19. ISO/IEC 27002:2013 (2013) Information technology – Security techniques – Information security management systems – Code of practice for information security management. ISO copyright office. Geneva, Switzerland.
20. ISO/IEC 27032:2012 (2012) Information technology — Security techniques — Guidelines for cybersecurity. ISO copyright office. Geneva, Switzerland.
21. Jennex M.E., Zyngier S. (2007) Security as a contributor to knowledge management success. *Inf Syst Front* 9(5):493-504.
22. Mansfield-Devine S. (2016) Securing small and medium-size businesses. *Netw Secur* 2016(7):14-20.
23. Mejjias R.J. (2012) An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk. In *proceedings of 2012 45th Hawaii International Conference on System Sciences*, p 3258-3267.
24. Miles I., Kastrinos N., Bilderbeek R., Den Hertog, P., Flanagan, K., Huntink, W., Bouman, M. (1995) Knowledge-intensive business services: users, carriers and sources of innovation. *European Innovation Monitoring System (EIMS) Reports*.

25. Morelli N. (2006) Developing new product service systems (PSS): methodologies and operational tools. *J Clean Prod* 14(17):1495-1501.
26. Mundbrod N., Reichert M. (2014) Process-aware task management support for knowledge-intensive business processes: findings, challenges, requirements.
27. NIST Special Publication 800-53 (2009) Recommended Security Controls for Federal Information Systems and Organizations Revision 3.
28. Nykänen R., Kärkkäinen T. (2016) Supporting Cyber Resilience with Semantic Wiki. In proceedings of OpenSym, 2016 ACM, New York, NY, USA, p 21:1–21:8.
29. Nykänen R., Kärkkäinen T. (2018) Tailorable Representation of Security Control Catalog on Semantic Wiki. In: Lehto M, Neittaanmäki P (eds) *Intelligent Systems, Control and Automation: Science and Engineering: Cyber Security: Power and Technology*, Springer.
30. Peffers K., Tuunanen T., Rothenberger M. A., Chatterjee, S. (2007) A Design Science Research Methodology for Information Systems Research. *J. Manage. Inf. Syst.* 24(3):45–77.
31. Pei Lyn Grace T. (2009) Wikis as a knowledge management tool. *Journal of knowledge management* 13(4):64-74.
32. Randeree E. (2006) Knowledge management: securing the future. *Journal of knowledge management* 10(4):145-156.
33. Renaud K. (2016) How smaller businesses struggle with security advice. *Computer Fraud & Security* 2016(8):10-18.
34. Rohn E., Sabari G., Leshem G. (2016) Explaining small business InfoSec posture using social theories. *Information and Computer Security* 24(5).
35. Royce W.W. (1970) Managing the development of large software systems. In proceedings of IEEE WESCON, vol 26. Los Angeles, p 328-338.
36. Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., Lindgren, R. (2011) Action Design Research. *MIS Q.* 35(1):37–56.
37. Shameli-Sendi A., Aghababaei-Barzegar R., Cheriet M. (2016) Taxonomy of information security risk assessment (ISRA). *Comput Secur* 57:14-30.
38. Siponen M. (2006) Information security standards focus on the existence of process, not its content. *Commun ACM* 49(8):97-100.
39. Spears J.L., Barki H. (2010) User participation in information systems security risk management. *MIS quarterly*:503-522.
40. Tatar Ü., Karabacak B. (2012) An hierarchical asset valuation method for information security risk analysis. In: 2012 International Conference on Information Society (i-Society).
41. Vaculin, R., Hull, R., Heath, T., Cochran, C., Nigam, A., Sukaviriya, P. (2011) Declarative business artifact centric modeling of decision and knowledge intensive business processes. In proceedings of Enterprise Distributed Object Computing Conference (EDOC), 2011 15th IEEE International IEEE, p 151-160.
42. Venable J.R. (2010) Design Science Research Post Hevner et al.: Criteria, Standards, Guidelines, and Expectations. In: Winter R, Zhao JL, Aier S (eds) Springer Berlin Heidelberg, p 109-123.
43. Venable J.R. (2015) Five and Ten Years on: Have DSR Standards Changed? In: Donnellan B, Helfert M, Kenneally J et al (eds) Springer International Publishing, p 264-279.
44. von Solms R., van Niekerk J. (2013) From information security to cyber security. *Comput Secur* 38:97-102.
45. Yeniman Yildirim E., Akalp G., Aytac S., Bayram, N. (2011) Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *Int J Inf Manage* 31(4):360-365.

VI

ANALYSIS OF THE NEXT EVOLUTION OF SECURITY AUDIT CRITERIA

by

Riku Nykänen, Tomi Kelo & Tommi Kärkkäinen 2023

Journal of Information Warfare, 22(4), 25-39

Reproduced with kind permission of Journal of Information Warfare.

Analysis of the Next Evolution of Security Audit Criteria

R Nykänen¹, T Kelo², T Kärkkäinen¹

¹*Faculty of Information Technology
University of Jyväskylä
Jyväskylä, Finland*

E-mail: riku.t.nykanen@student.jyu.fi; tommi.p.karkkainen@jyu.fi

²*Department of Pervasive Computing
Tampere University of Technology
Tampere, Finland*

E-mail: tomi.kelo@tuni.fi

Abstract: *Security assessments are performed for multiple reasons, including compliance with the information security regulation. Amongst other objectives, regulatory requirements are created to increase the resilience of national infrastructure and protect against information and cybersecurity threats. When the regulatory requirements are revised, the security audit criteria also need to be updated and validated. This was also the case with the Julkri, criteria developed for the conformance assessments of the renewed Finnish information security regulation. In this article, a comparative evaluation based on Design Science Research is performed to determine whether the new Julkri criteria improve existing criteria and control catalogues.*

Keywords: *Security Audit Criteria, Security Assessment, Information Security Controls, Design Science Research*

Introduction

Security controls are countermeasures that an organization implements to mitigate specific security risks. Security controls can be administrative, such as policies, processes, and training, or technical, such as endpoint protection software and backups. Organizations should implement cost-effective controls based on the risk assessment to mitigate their information and cybersecurity risks. The implemented controls are typically selected from a security control catalogue, which can be described as collections of the best practices for mitigating common information and cybersecurity risks.

Information security audits are used to assess the adequacy of organizations' information security from the compliance point of view. In the audits, a security control catalogue, such as ISO/IEC 27002 (International Organization for Standardization 2022b), NIST SP 800-53 (National Institute of Standards and Technology 2020), CIS Controls (Center for Internet Security 2021), or Katakri (National Security Authority of Finland 2020), defines the criteria that an organization is expected to meet. Security control catalogues are also regularly used when organizations assess their service providers or subcontractors to ensure the security of their supply chain.

The selection of used audit criteria and the security control catalogue are usually defined based on the security assessment. As an example, ISO/IEC 27002 is a widely adopted international standard by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) used as a part of ISO/IEC 27001 certification audits. As another example, NIST SP 800-53 is a U.S. national standard by the National Institute of Standards and Technology (NIST). The CIS Controls by the community-driven non-profit organization Center for Internet Security (CIS) is an example of a widely adopted reference control set without a status as a national or international standard. The Finnish Information Security Audit Tool Katakri is also a noteworthy example, being created in close cooperation between Finnish governmental security authorities and the private sector, with a focus on the protection of national classified information.

As organizations are different, management of information and cybersecurity is often risk-based, aiming to find the optimal controls for the current organization, the currently protectable assets, and/or a more strictly specified use case (Calvo & Beltrán 2022). Security risk management methodologies usually contain similar common phases (Fenz & Ekelhart 2011), where one essential phase is to analyse and select controls to mitigate the identified risks. For example, ISO/IEC 27001 requires an organization to “determine all controls that are necessary to implement the information security risk treatment option(s) chosen” and compare selected controls to ISO/IEC 27002, so that no necessary controls have been omitted. The risk-based approach allows the use of a control catalogue as a support mechanism to identify potential security controls. Performing effective risk identification, assessment, and mitigation for all assets seems to be extremely challenging even for organizations with adequate resources (McKeown 2019).

Where the private sector may have more freedom in the selection of suitable audit criteria for the specific purpose, the public sector is often more constrained to comply with the regulatory requirements. In this article, the authors analyse the process and outcomes of Julkri criteria (Information Management Board 2022) development using Design Science Research (Peffer *et al.* 2007). Julkri criteria were developed to provide a new tool for the conformance assessments of the renewed Finnish information security regulation, the Act on Information Management in Public Administration (906/2019) (Parliament of Finland 2019a), and the Government Decree on Security Classification of Documents in Central Government (1101/2019) (Parliament of Finland 2019b).

Security Audit Criteria and Control Catalogues

Security assessment

Compliance can be defined as the process of meeting expectations. More specifically, compliance is “verifiable consistency with clearly defined rules” (DeLong 2014). An information security assessment is the evaluation process to verify compliance against a set of rules. The set of rules is defined by the evaluation criteria used in the assessment. Information security audits can have multiple types of targets from organizations to specific products. Where the ISO/IEC 27001 (International Organization for Standardization 2022a) standard is a requirement specification for an Information Security Management System (ISMS), other specifications originate, for example, from regulatory or technical backgrounds. Hence, it is important to select a control catalogue adequate for the assessment.

The development, or update cycles, of security control catalogues occur typically in intervals of a few years. For example, the three versions of ISO/IEC 27001 were published in 2005, 2013, and 2022, and the last three versions of NIST SP 800-53 were published in 2009, 2014,

and 2019. Although the cybersecurity landscape evolves rapidly, the current update intervals of security control catalogues support the assessment purpose by improving stability in the requirements. Faster criteria update cycles could lead to an extra burden if the recertification interval is too stringent. Hence, updates to security control catalogues usually have accumulated needs for changes over several years.

When developing a new security control catalogue, there is no need to reinvent the wheel as several catalogues already exist. However, a rationale for a new catalogue is required. In the case of Julkri, the rationale was based on the need for compliance assessments against the updated regulations. With such a rationale, the content of the criteria must meet the regulatory requirements, although the basis for criteria can be formed from already existing specifications.

The semantics of security control catalogues

Security control structures vary in different frameworks. **Table 1** summarizes the previously presented control catalogue structures: NIST SP 800-53 release 5, ISO/IEC 27002:2022, CIS Controls v8, and Katakri 2020. The rationale for framework selection, instead of, for example, MITRE D3FEND, NIST Cybersecurity Framework, and BSI IT Grundschutz, is based on recent structural advancements of the selected frameworks.

	NIST SP 800-53 rel 5	ISO/IEC 27002:2022	CIS Controls v8	Katakri 2020
Control basic information	Identifier Name Control (text)	Identifier Name Control (text)	Controls: Number Title Safeguards: Number Title	Identifier Title Requirement(s)
Description	Discussion	Purpose Guidance Other information	Controls: Overview Why is this control critical? Safeguards: Description	Examples of implementation (as part of additional information)
References	External references Related controls			Legal references Other sources of information (as part of additional information)
Sub elements	Control enhancements		Safeguards	
Other attributes	Status (active or withdrawn)	Control type Information security properties Cybersecurity concepts	Controls: Procedures and tools Safeguards: Asset type	

		Operational capabilities Security domains	Security function Implementation group	
--	--	--	---	--

Table 1: Structural elements of security control catalogues

All selected catalogues have the following common basic elements for security controls: a unique identifier, control title, and description. ISO/IEC 27002:2022 has added five new attributes to controls compared to the previous version: control type, information security properties, cybersecurity concept, operational capabilities, and security domains. Attributes are intended to be used to create different views of a control catalogue to select appropriate subsets of controls.

A control type attribute describes how and when a control impacts the risk outcome and has the following possible values: *preventive*, *detective*, and *corrective*. The control type attribute is information that overlaps somewhat with the cybersecurity concept attribute, which can have the values identify, protect, detect, respond, and recover defined in the ISO/IEC TS 27101 “Cybersecurity framework development guidelines” standard draft and already implemented in the NIST Cybersecurity Framework. The information security properties define which information security properties, that is, confidentiality, integrity, and availability (CIA), are protected by the corresponding control (Yee & Zolkipli 2021).

The security domain is an attribute to view controls from the perspective of information security fields, expertise, services, and products. Attribute values consist of the following: *Governance and Ecosystem*, *Protection*, *Defence* and *Resilience*. The attribute is based on the needs of the European Union Directive 2016/1148 (also known as the NIS directive). The directive defines cybersecurity requirements for specific critical domains. The European Union Agency for Cybersecurity (ENISA) has produced equivalent mapping to ISO/IEC 27001 requirements and Annex A with the same attribute values. The operational capabilities describe aspects of the security operations, which are valid for the specific security controls. There are 14 possible values, including *Governance*, *Asset Management*, *Information Protection*, *Human Resource Security*, and *Physical Security*. The objective of the attribute is to be able to filter controls from the practitioner’s perspective.

ISO/IEC 27002:2022 and CIS Controls include an additional shared attribute. CIS Controls include a *security function* attribute for each safeguard to define how the safeguard supports cybersecurity. Possible values, originally defined in the NIST Cybersecurity Framework (Barrett 2018), are as follows: *identify*, *detect*, *protect*, *recover*, and *respond*, where one of the values is set for each safeguard. ISO/IEC 27002:2022 has an attribute called *cybersecurity concept* that has the same values, but each control can have multiple values selected. CIS Controls also define attribute named asset type that describes the types of assets the corresponding safeguard protects. Asset taxonomy includes the following types: *Applications*, *Data*, *Devices*, *Network*, and *Users*, but some of the safeguards do not apply to every asset type (marked as N/A). Although the asset taxonomy is simple, it can be used similarly to the way ISO/IEC 27002:2022 uses operational capabilities.

The CIS Controls’ structure differs from the other analysed frameworks in a significant way. Security control in CIS Controls can be seen as a high-level objective to ensure security in a specific function. Security control is, however, extended with definitions of multiple safeguards for each control. Safeguards can be characterized as more concrete activities to

ensure the objective defined by the security control. Safeguards are at a similar level as security controls in the other analysed frameworks. A similar high-level control objective was used in the previous versions of ISO/IEC 27002 but was removed from the 2022 version.

Like CIS controls, NIST SP 800-53 and Katakri have similar two-level approaches. NIST SP 800-53 controls have control enhancements, which can be seen as sub-controls, as they are structurally nearly the same as controls. Control enhancements always belong to specific security controls. Katakri has implemented levels within requirements in textual format and does not have similar structural elements. A single criterion (control) in Katakri can have multiple security requirements, but some of the requirements apply only to a certain security classification level. All three frameworks have implemented prioritization of security controls utilizing the presented structures. Where all controls are not applicable on all security or risk levels, the two-level approach enables primary control to be always active and applying the sub-elements only on suitable security levels.

Methods

The development of new Julkri criteria contained elements that resemble the Design Science Research (DSR) process. Although Julkri development did not claim to use DSR as a development framework during the project, the authors will evaluate the developed artefact based on DSR evaluation criteria. DSR is a research method that is used to develop a set of artifacts to solve a wicked problem. The iterative DSR process is composed of relevance, rigor, and design cycles (Hevner 2007) as presented in **Figure 1**.

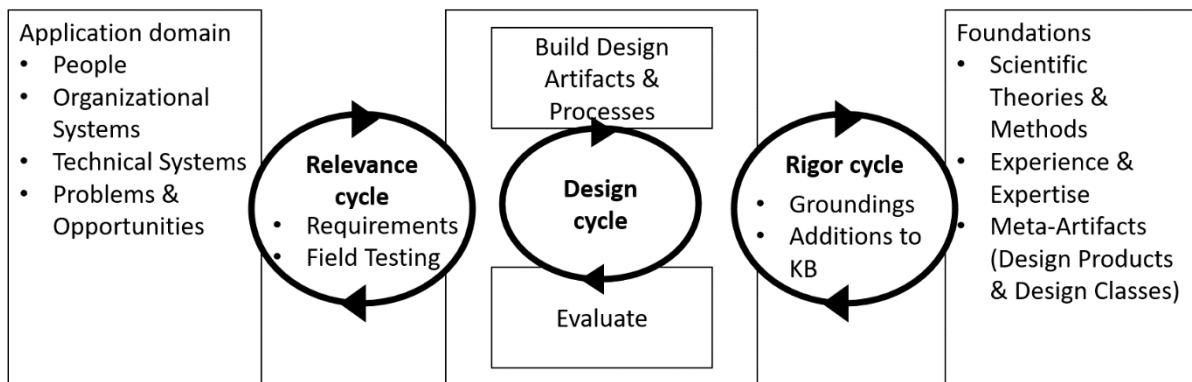


Figure 1: Design Science Research cycles (Hevner 2007)

The relevance cycle ensures that technology-based solutions solve important and relevant business problems, setting the requirements and acceptance criteria for research results. The rigor cycle provides the prior scientific knowledge and theories as a foundation for the research but also ensures that rigorous methods are applied in the construction and evaluation of the artifact. The design cycle research activities iterate between the construction of an artifact, its evaluation, and feedback to refine the design further (Hevner 2007).

In the Julkri development, the rigor cycle included the evaluation of recent development of related standards and methods. At the time of Julkri work, ISO/IEC 27002 version 2022 reached the approval stage where the Final Draft International Standard (FDIS) version was available for analysis. In addition to ISO/IEC 27002, also recently published NIST SP 800-53 release 5 was analysed in a rigor cycle for structural elements that could be used in Julkri. Where the rigor cycle concentrated on the structure, the relevance cycle focused more on the content of the Julkri criteria. Julkri's requirements are based on the legislation. Thus, the content

of the criteria is not expected to be equal to international standards or best practices as they contain security controls not arguable by legislative requirements. Still, the criteria must consider security controls usually expected to be implemented to ensure the information security requirements of the legislation.

As Julkri development contains typical elements of a DSR project to solve a wicked problem of legal conformance, the developed criteria shall be evaluated as a DSR artefact. DSR as a research method can have multiple goals, which require different evaluation strategies. Framework for Evaluation in Design Science (FEDS) addresses the lack of guidance to evaluate DSR research (Venable, Pries-Heje & Baskerville 2016). The authors utilize FEDS to create evaluation strategies to perform a comparative evaluation to determine if Julkri, as a DSR artifact, is an improvement, compared to other existing criteria and control catalogues. As evaluation is performed *ex-post* concerning the Julkri development; the summative evaluation strategy is used. Evaluation episodes are based on the DSR research goals (Venable 2010), which are complemented by security audit criteria evaluation principles (Kelo, Eronen & Rousku 2018). The authors utilize the Quick and Simple evaluation strategy, suitable for summative *ex-post* evaluation (Venable, Pries-Heje & Baskerville 2016). The Model for Efficient Development of Security-Audit Criteria (Kelo, Eronen & Rousku 2018) includes three phases of criteria development: design, implementation, and utilization. As the authors evaluate only Julkri as an artefact, the utilization phase from evaluation is excluded and the authors focus instead on the design and implementation phase.

Development of Julkri Criteria

Regulatory background

As multiple security control catalogues already exist, including national Katakri and PiTuKri (Finnish Transport and Communications Agency Traficom 2020), the need for Julkri was not evident. The rationale for Julkri development was based on the authoritative role and tasking of the National Information Management Board (IMB) (Information Management Board 2023).

As the IMB has the responsibility to define procedures based on the Act on Information Management in Public Administration, Julkri criteria were developed for compliance assessments. Regulatory requirements are generally written on a high abstraction level, which is not optimal for compliance assessments. To support the assessments, the criterion needs to refine the requirements on a more detailed level. These refinements were based on controls defined in standards and other best practices.

Julkri criteria content was initially based on Katakri and additionally on cloud security assessment criteria PiTuKri. The regulatory background of the latest Katakri version is the same as in Julkri (906/2019 and 1101/2019), focusing on the protection of classified information on levels RESTRICTED, CONFIDENTIAL and SECRET. Katakri also covers the protection of European Union Classified Information (EUCI). Scope for Julkri excluded protection of EUCI but included national TOP SECRET.

Development process

In the initial development cycles, activities of relevance and rigor cycles were executed in parallel. The initial version of criteria content was developed by the groups of subject experts as part of relevance and design cycles. The structure of the criteria was developed in the rigor cycle by the core development team. As the development work proceeded, more focus was on relevance and design cycles and less was on rigor cycles.

The initial content of Julkri was based on the Katakri with cloud security supplements from PiTuKri. Compared to the Katakri sections, new sections of “Preparedness and continuity management” and “Personal data protection” were introduced. After completion of the initial content, legislative validation was performed. At this phase, the phrasing of multiple criteria and recommendation texts was modified to meet the regulatory requirements more precisely.

The draft recommendation was open for comments via the public commenting service after legislative validation. Both public and private organizations were invited to provide their statements for the Julkri draft. In total, 32 organizations provided their responses to the proposal. Of these, 23 were public sector organizations, including, for example, municipalities, ministries, and government agencies. Seven of the responses were from private sector companies, including, for instance, global cloud service providers.

In general, the feedback was positive. Multiple responses indicated that criteria clarify the assessment of regulatory requirements. Also, the structure of the criteria and language used were found to be clear. In negative feedback, two issues were emphasized. First, the relationship and priority between the three different national criteria (Julkri, Katakri, and PiTuKri) was not seen to be clear. Secondly, the support for zero trust architecture was not seen as sufficient. Based on the feedback, the criteria were slightly modified. The structure and metamodel of Julkri did not receive negative feedback and were thus not modified.

Structure of Julkri

The final structure of the Julkri criteria can be divided into two main elements: the Julkri guideline document and the Julkri tool. The Julkri guideline document is composed of the following elements:

- Recommendation document - Background and guidelines on how to use Julkri
- Annex 1A - List of criteria as the text document
- Annex 1B - List of personal data protection criteria as the text document
- Annex 2 - Julkri tool (spreadsheet, not included in the document)
- Annex 3 - Julkri tools guideline
- Annex 4 - Glossary

Annex 1 was separated into two parts, 1A and 1B, after another legislative validation. The rationale was based on competencies; only the Office of the Data Protection Ombudsman (ODPO) is authorized to provide guidance on personal data protection in Finland. Hence, the domains under IMB and ODPO competencies were separated. The second main element of Julkri is the Julkri tool, which is an Excel spreadsheet. It contains criteria defined in Annex 1A and 1B in format, where criteria can be filtered based on preconditions. Preconditions are based on the criteria metamodel.

Criteria metamodel

Open Security Controls Assessment Language (OSCAL) defines a generic metamodel of control catalogues, control baselines, system security plans, and assessment plans and results. NIST SP 800-53 revisions 4 and 5 have been published in OSCAL format. In Julkri development, Katakri was used as a basis for the metamodel and hence OSCAL was not followed but was used in the evaluation. The Julkri metamodel and its comparison to OSCAL concepts are presented next.

The complete Julkri tool consists of five sections as described earlier, which each contain a set of criteria. Each criterion can have an additional sub-criterion to provide more detailed requirements or implementation guidance. This structure was adopted from NIST SP 800-53, which has a similar two-level control and control enhancement structure. In the initial version, it was allowed to have a recursive hierarchy of sub-criterion. It was however identified at a very early phase that a two-level structure was sufficient and easier to understand. Criterion and sub-criterion are structurally identical with the exception that the sub-criterion has additional reference to the parent criterion. It should be noted that all attributes are not mandatory, and many sub-criterions provide, for example, only additional implementation guidance for higher security levels. The attributes of a criterion are presented in **Table 2**.

Element	Description
Identifier	A unique identifier consisting of the abbreviation of the name of the sub-area, a consecutive number of the main criterion and, in a sub-criterion, also a consecutive number of the sub-criterion.
Name	The subject of the criterion
Requirement	The objective that the organization must meet. The requirement is a short sentence or a short paragraph.
Overview	Additional information that provides background and justification for the criterion.
Implementation guidance	Description of how the organization can implement the requirement. An implementation example is not a requirement, but it can serve as a guideline for the level of compliance with the requirement.
Confidentiality	Minimum confidentiality level when the criterion is expected to be applied.
Integrity	Minimum integrity level when the criterion is expected to be applied.
Availability	Minimum availability level when the criterion is expected to be applied.
Privacy	Minimum privacy level when the criterion is expected to be applied.
Legislation	The legislation on which the criterion is based.
References	References to the recommendations by the IMB, the PiTuKri assessment criteria and standards, including ISO/IEC 27002.
Julkri reference	A reference to one or more other relevant Julkri criterion.
Katakri reference	A reference to the corresponding criterion in the Katakri, if one exists.

Table 2: The attributes of a Julkri criterion

From these elements, confidentiality, integrity, availability, and privacy are later referred to as CIAP properties. During the rigor cycle, an analysis of existing classifications, especially for integrity and availability, were conducted, and the scale was implemented based on the findings. For confidentiality and privacy, scales were already defined in the legislation. **Figure 2** presents the Julkri metamodel as a UML diagram.

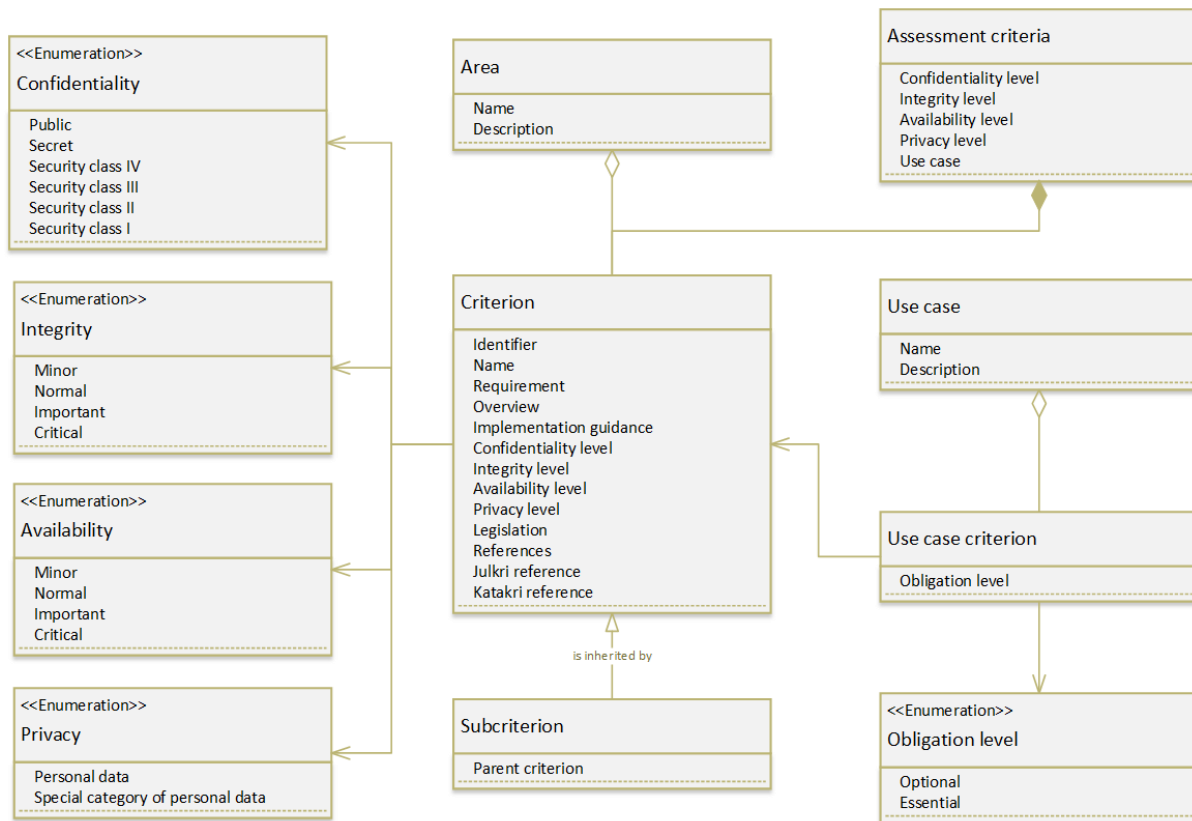


Figure 2: Julkri metamodel

OSCAL concepts were analysed in the rigor cycle as one input for the meta-model design. The concept of profiles had an especially significant impact on the use case concept of Julkri. **Table 3** presents a mapping of Julkri concepts to OSCAL concepts.

OSCAL concept	Julkri concept
Catalog	Criteria
Profile	Use case
Group (Family)	Area
Control	Criterion
Control enhancement	Sub-criterion

Table 4: Mapping of OSCAL and Julkri concepts

The global or control parameters concepts of OSCAL, as utilized in NIST SP 800-53 rev 5, were not included in Julkri. The rationale is two-fold: Julkri is not expected to be utilized by other specifications, but to be adapted via use cases. On the other hand, the functionality of control parameters is implemented using sub-criterion refining the main criterion.

Adapting a risk-driven approach

Applying regulatory requirements for a risk-driven approach was analysed during the rigor cycle. As a result, OSCAL control layer concepts were used to implement the risk-driven approach. Compared to Katakri and PiTuKri, utilizing only the confidentiality of information as selection criteria, Julkri's approach was more versatile.

First, Julkri’s concept of use case is like the OSCAL profile and NIST Risk Management Framework concept of overlays. Julkri use cases are used to define a subset of criteria that is relevant to a specific purpose. The OSCAL profile is a binary approach to include or exclude a control from a profile. However, in Julkri, the use cases have three options: essential, optional, or excluded. Essential criteria are considered mandatory to be complied with, but they can be compensated with other controls. Each optional criterion shall be evaluated based on risk—to be included in the assessment or not. Excluded criteria are scoped out.

In addition to the predefined use cases, customised use cases can also be defined. The first version of Julkri criteria contains four common use cases:

- Public Administration Unit security assessment
- SaaS cloud service security assessment
- Professional services security assessment
- IT service provider security assessment

The risk-driven approach is implemented in Julkri using use cases and CIAP properties, which are used as input for criteria selection. Selection logic is shown in **Figure 3**.

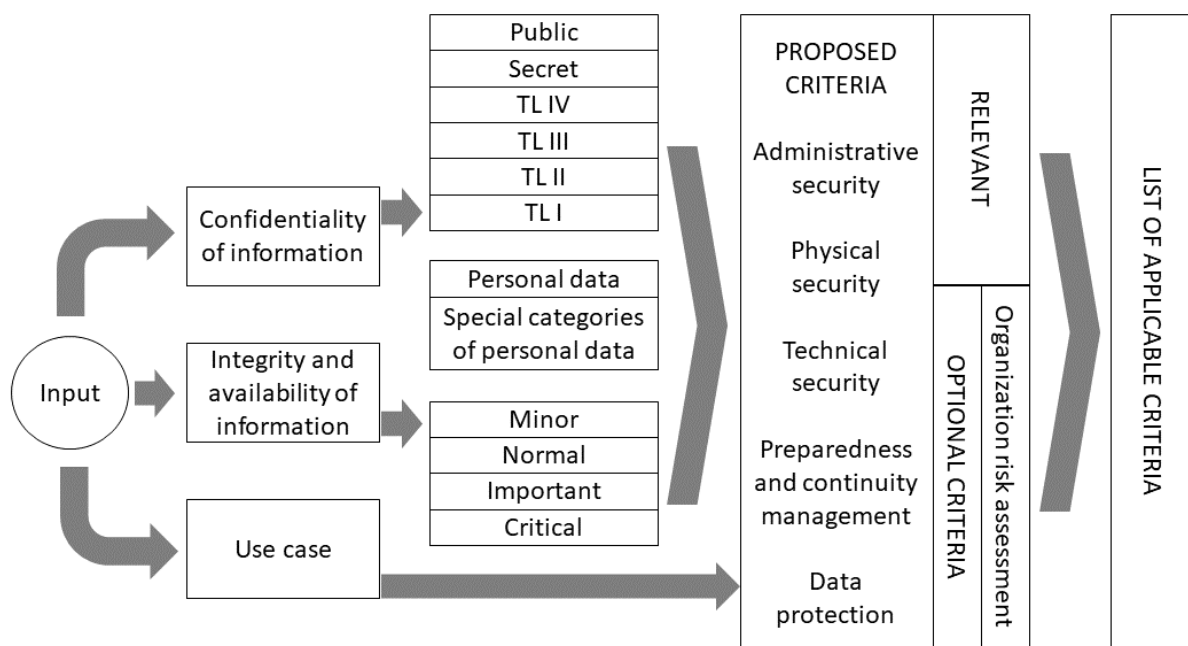


Figure 3: Illustration of selecting the applied criteria (Information Management Board 2022)

The number of essential criteria is fairly small compared to the number of optional criteria as it requires both the use case and CIAP property to be essential for the criterion. Criterion will be optional if CIAP property or use case is optional. Criterion is excluded only if none of the properties is essential or optional. This approach emphasizes the necessity of risk assessment to select the optimal set of security controls to be implemented.

Validation of criteria

During the finalization of the criteria, the coverage of contents was analysed against ISO/IEC 27001, ISO/IEC 27002, and PiTuKri. The purpose of the validation was to ensure that Julkri is not lacking essential requirements. Analysis can be considered as “triad verification”, as regulatory requirements were also considered while evaluating correspondence. For example,

ISO/IEC 27002:2022 contains several security controls that are not covered by Julkri due to a lack of regulatory requirements. Additional verification was also performed against Katakri to ensure that no essential original Katakri content had been deleted or modified during the development process.

Evaluation of Julkri artefact

Next, the authors evaluated Julkri against design (IDs 1-3) and implementation (IDs 4-10) phase guidelines (Kelo *et al.* 2018). Utilization phase guidelines (IDs 11-16) are partially outside of the scope of the development project but are included in the analysis when applicable.

ID 1: Criteria design should stem from a small set of carefully selected and strictly defined use cases.

The guideline defines that criteria should limit the number of supported use cases and target groups to avoid balancing between requirements of different use cases and interests leading to a useless assessment tool. It is evident that the approach of Julkri is different from the evaluation guideline. By introducing a use case as a structural element and utilizing control selection using CIAP properties, Julkri can be adapted to multiple use cases and supports user organizations to adopt it to their specific use cases. As Julkri's use case is based on the OSCAL concept of overlays, it can be argued that is this a false negative finding as a similar approach is used also in the other criteria (Venable, Pries-Heje & Baskerville 2016).

ID 2: Use cases should be defined early in the criteria-development process. The validity of use cases should be ensured throughout the process.

Like guideline ID 1, Julkri's approach is different. Where its successors Katakri and PiTuKri have strictly defined use cases, Julkri contains more requirements from which a subset can be selected for a specific use case.

ID 3: Criteria should have an understandable scope and a reasonable number of requirements.

The scope of Julkri is to assess the fulfilment of the information security requirements laid down in the Information Management Act, Security Classification Decree, and partly also in the General Data Protection Regulation. Feedback from the public commentary period indicated that the relationship and status compared to other existing criteria was not clear, also indicating possible shortcomings in scope definitions and guidance on the proper use of the criteria.

ID 4: Common risks related to the use cases should be identified. The required controls should cover these risks.

The initial content of Julkri was based on the established Katakri and PiTuKri frameworks, and the content was also verified against ISO/IEC 27001 and ISO/IEC 27002:2022 standards. As some of the supported use cases are similar, also many of the use case specific risks are expected to be similar, and thus sufficiently covered. This does not however guarantee that all risks related to all use cases would be covered.

ID 5: Security criteria should describe minimum requirements but should also provide support for the security and risk-management processes of the target groups.

Julkri makes a noteworthy enhancement to the risk-driven approach by introducing a logic to select the minimum and optional risk-based requirements. The approach requires competence in risk management to select valid optional requirements. Without sufficient competence, the

approach may lead to unwanted situations. As an example, an organization may only comply with mandatory minimum requirements, and fail to identify a need for additional controls even in high-risk use cases. The development process did not include testing with various user organisations, emphasizing the need for further analysis after practical usage.

ID 6: Each criteria requirement should be justifiable for the use cases.

All requirements were formulated by groups of subject matter experts and were based on established frameworks. From the DSR perspective, the public comment period can also be seen as a verification method to avoid, for example, biased views by experts or other criteria. In the case of Julkri, the comments did not include feedback that any requirement would be obsolete or not justifiable for the use cases.

ID 7: Requirements should be described at a reasonably concrete abstraction level.

Julkri's content was based on existing established criteria and standards, including the selected level of abstraction. Feedback gathered from the public commentary indicated the need for only a few clarifications.

ID 8: Criteria should be internally consistent.

Julkri's approach was to use requirements from established existing criteria and to split the requirements into more atomic requirements where appropriate. The approach enabled cross-referencing and comparison of the requirements on an atomic level. The approach made also internal inconsistencies clearly visible and effectively fixable.

ID 9: Authoritative sources should be referenced clearly.

As the meta-model shows, Julkri contains references to regulatory sources of requirements. Also, the authoritative role of the IMB was clearly stated in the criteria.

ID 10: The requirements should be compared to those of similar criteria to reveal possible biases.

Requirements were based on established similar criteria and were also verified against similar criteria and standards. Although no noteworthy biases were identified, the remark was made on non-similar use cases in criteria and standards selected for comparison, which may leave some biases unnoticed.

ID 11: Thorough practical testing of the criteria should be conducted before publication.

Julkri's development did not include an extensive practical testing phase. As Julkri was mainly based on an established, extensively tested Katakri framework, it was expected that no major findings would have been found in the practical testing of Julkri. On the other hand, Julkri also introduced support for use cases not supported in Katakri, and testing such use cases might have been justified.

ID 13: Instructions for proper usage within each of the use cases should be provided.

Julkri has extensive guidelines included as part of the main document release. In addition to guidance included in the recommendation document, the document has also Appendix 3, which includes instructions on how to use the Julkri Excel tool.

ID 14: Appropriate guidance and training should be offered to unify the interpretation of criteria.

At the time of publishing Julkri, there was no training material available. The development of training material, however, began after the publication.

ID 16: Criteria should be made available to the target groups.

Julkri is publicly available on IMB's website, free of charge.

Themes covered in guidelines ID 12 (Effort should be expended to gain recognition for the criteria) and ID 15 (Audits of critical targets should be limited to certified practitioners to ensure sufficiently reliable results) were outside of the scope of the Julkri development and were thus not evaluated in this research.

Results and discussion

Summary of the results:

- The use of established frameworks can operate as an efficient starting point for new criteria.
- The designed metamodel of Julkri supports several enhancements compared to many existing frameworks. As an example, a risk-driven approach can be supported by introducing a logic to select the minimum and risk-based additional controls. As another example, the amount and variety of supported use cases may be flexibly expanded by metamodel design and atomicity of criteria requirements.
- The public comment period is an essential method to verify the applicability of DSR artefacts to real-world scenarios.
- The Julkri development process did not include testing with various user organisations, emphasizing the need for further analysis after practical usage.

When considering criteria development guidelines ID 1 and ID 2, the security control catalogues and security audit criteria can be divided into two categories: general catalogues and use case specific catalogues. General catalogues can be adapted for use case specific needs using approaches like OSCAL profiles and control parameters while supporting many use cases. Further research is needed to analyse whether the use case specific approach provides a more understandable and practically efficient tool for various user groups, or whether similar results can be achieved with adapted general catalogues.

When evaluating guidelines ID 11, ID 13, and ID 14, it seems evident that the development of Julkri criteria should have included practical testing as well as the creation of training materials. If Julkri is being taken into practical use by the target groups, their experiences could provide valuable input for further research. Future research topics could focus especially on utilization phase guidelines (IDs 11-16), and could cover, for instance, efforts made to gain recognition of the criteria (ID 12). Analysis of ID 12 would be needed especially if the Julkri criteria is being taken into practical use parallel or in conjunction with the other established frameworks.

Future research would also be needed on the practical implementations of the risk-driven approach. The introduced logic to select the minimum and risk-based additional controls especially requires further validation. A validation is recommended in practical use cases, covering the soundness of the logic, understandability for the users, and the sufficiency of resulting protection against security risks currently faced by user organisations.

References

- Barrett, M 2018, 'Framework for Improving Critical Infrastructure Cybersecurity', version 1.1, *NIST Cybersecurity Framework*, National Institute of Standards and Technology, Gaithersburg, MD, US.
- Calvo, M & Beltrán, M 2022, 'A model for risk-based adaptive security controls', *Computers & Security*, vol 115.
- Center for Internet Security 2021, *CIS Critical Security Controls*, 8th ed, viewed 20 February 2023, <<https://www.cisecurity.org/controls>>.
- DeLong, J 2014, 'Aligning the compasses: A journey through compliance and technology', *IEEE Security & Privacy*, vol. 12, no. 4, pp. 85-9.
- Fenz, S & Ekelhart, A 2011, 'Verification, validation, and evaluation in information security risk management', *IEEE Security & Privacy*, vol 9, no. 2, pp. 58-65.
- Finnish Transport and Communications Agency Traficom 2020, *Criteria to Assess the Information Security of Cloud Services (PiTuKri)*, edition 1.1, ISBN 978-952-311-505-7, Traficom publications, Helsinki, Finland.
- Hevner, AR 2007, 'A three-cycle view of design science research', *Scandinavian Journal of Information Systems*, vol. 19, no. 2, pp. 87-92.
- Information Management Board 2022, *Assessment criteria for information security in public administration (Julkri): Recommendation and criteria*, 1st ed., Publications of the Ministry of Finance, Ministry of Finance, Helsinki, Finland.
- 2023, Ministry of Finance, viewed 20 February 2023, <<https://vm.fi/en/information-management-board>>.
- International Organization for Standardization 2022a, *Information security, cybersecurity and privacy protection, Information security management systems, Requirements*, ISO 27001:2022 edition, International Organization for Standardization, Geneva, Switzerland.
- 2022b, *Information security, cybersecurity and privacy protection—Information security controls*, ISO 27002:2022 edition, International Organization for Standardization, Geneva, Switzerland.
- Kelo, T, Eronen, J & Rousku, K 2018, 'Enhanced model for efficient development of security-audit Criteria', *Journal of Information Warfare*, vol. 17, no. 3, pp. 50-63.
- McKeown, DA 2019, 'Building a risk-based information security culture', *ISSA Journal*, vol. 17, no. 4, pp. 14-21.
- National Institute of Standards and Technology 2020, *Security and Privacy Controls for Information Systems and Organizations, Special Publication 800-53*, 5th ed., National

Institute of Standards and Technology, Gaithersburg, MD, US.

National Security Authority of Finland 2020, *Katakri 2020: Information Security Audit Tool for Authorities*, ISSN 2669-8757, Finnish Transport and Communications Agency Traficom, Helsinki, Finland.

Parliament of Finland 2019a, *Act on information management in public administration (906/2019)*, Ministry of Finance, Finland, viewed 20 February 2023, <<https://www.finlex.fi/en/laki/kaannokset/2019/en20190906.pdf>>.

—2019b, *Government Decree on Security Classification of Documents in Central Government (1101/2019)*, Ministry of Finance, Finland, viewed 20 February 2023, <<https://www.finlex.fi/en/laki/kaannokset/2019/en20191101.pdf>>.

Peffer, K, Tuunanen, T, Rothenberger, MA & Chatterjee, S 2007, 'A design science research methodology for information systems research', *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45-77.

Venable, J, Pries-Heje, J & Baskerville, R 2016, 'FEDS: A framework for evaluation in design science research', *European Journal of Information Systems*, vol. 25, no. 1, pp. 77-89.

Venable, J 2010, 'Design science research post Hevner *et al.*: Criteria, standards, guidelines, and expectations', *Global Perspectives on Design Science Research, DESRIST 2010, Lecture Notes in Computer Science*, eds. R Winter, JL Zhao & S Aier, Springer, Berlin, Heidelberg, Germany, pp. 109-23.

Yee, CK & Zolkipli, MF 2021, 'Review on confidentiality, integrity and availability in information security', *Journal of ICT in Education*, vol. 8, no. 2, pp. 34-42.