Mapping the State of Security Standards Mappings

Andrea Mussmann[1], Michael Brunner[1], Ruth Breu[1]

[1] University of Innsbruck, Department of Computer Science, Innsbruck, Austria
{firstname.lastname}@uibk.ac.at

Abstract. Companies often have to comply with more than one security standard and refine parts of security standards to apply to their domain and specific security goals. To understand which requirements different security standards stipulate, a systematic overview or mapping of the relevant natural language security standards is necessary. Creating such standards mappings is a difficult task; to discover which methodologies and tools researchers and practitioners propose and use to map security standards, we conducted a systematic literature review. We identified 44 resources published between 2004 and 2018 using ACM Digital Library, IEEEXplore, SpringerLink, ScienceDirect, dblp and additional grey literature sources. We found that research focuses either on manual methods or on security ontologies to create security standards mappings. We also observed an increase in scientific publications over the investigated timespan which we attribute to the ISO 27001 standard update in 2013 and the EU GDPR coming into effect in 2018.

Keywords: Security Requirements, Security Standards, Security Mapping, Compliance Management, Systematic Literature Review.

1 Introduction

Information security standards, frameworks and guidelines support companies to secure their business processes and to obtain certification from standards organisations or government agencies and thus play an important role in information security [1]. Prominent information security standards include COBIT [2], the ISO 27000 [3] family of standards, or the PCI-DSS [4]. Information security standards (abbreviated to *standard* within the scope of this paper) collect heterogeneous security requirements covering organizational practices, processes and many directly or indirectly related aspects which organisations have to fulfil. These documents are potentially very large bodies of natural language text.

Companies may want to or have to comply with more than one such standard. Standards might overlap (i.e. implementing one standard leads to a partial fulfillment of another standard), complement but also contradict each other. In order to understand how two or more standards are related, standards mappings are created. Mapping tables are an important support-tool for a broad set of compliance management activities. They list security requirements of one standard and their equivalents in the other standard(s) or show potential conflicts between them.

15th International Conference on Wirtschaftsinformatik,
March 08-11, 2020, Potsdam, Germany

https://doi.org/10.30844/wi_2020_l4-mussmann

However, since standards are (potentially very large) natural language texts, creating and maintaining such mappings manually requires a lot of effort, especially if standards are defined for different contexts (e.g. general information security management like ISO 27001 [3] vs. dedicated information security requirements for online payment services like PCI-DSS [4]). Furthermore, taking the often evolutionary character of security standards into account, procedures to reliably and efficiently maintain mappings throughout standard revisions are desirable. This raises the question of how mapping tables are currently created and for which standards such mapping tables exist.

An initial investigation to find systematic literature reviews on the topic of standards mapping yielded no satisfactory results. Haufe et al. [5] base their observation on a non-systematic review searching for security standards mapping under the aspect of information security management system processes and quickly proceed to propose such a process mapping themselves. In [6], Olifer evaluates proposed standards mapping methodologies. He does identify four different techniques of standard mapping initially, but then exclusively focuses on an adaptive mapping approach based on ontologies.

This paper presents a systematic literature review that gives an overview of research on mapping security standards. It provides a survey of existing standards mappings created by researchers, as well as standards and commercial organisations, and finds methodologies developed for the creation of such mappings. Our review also investigates tool-supported techniques developed by researchers. From our findings, possible directions for further research in the area of security standards mapping are derived.

The remainder of this paper is structured as follows. The methodology of the systematic literature research as well as the research questions are presented in Section 2. The results of the review are presented and used to answer the research questions in Section 3. We conclude our paper and outline promising future research directions in Section 4.

2 Methodology

The creation of security standards mappings is relevant both in research and in practice. A literature study in this area thus has to take into account grey literature as well as scientific, peer-reviewed publications. In order to capture both the state-of-the-art and state-of-practice in security standards mappings, we conducted a multivocal systematic literature review based on the best-practice guidelines of Kitchenham [7] and Garousi et al. [8]. As there exists no systematic literature review on the topics of security standards mapping or security standards mapping methodology, the research questions are:

RQ1: For which pairs of security standards do mappings exist and who creates and publishes security standards mappings?

https://doi.org/10.30844/wi_2020_l4-mussmann

RQ2: How, both in terms of methodology and degree of automation, are security standards mappings created?

Since this literature review cannot give a complete overview of all available security standards [9], a selection of the most popular information security standards according to the ranking in [9] has been made. The standards ISO/IEC 27001 and ISO/IEC 27002 [3], PCI-DSS [4], the NIST SP-800 series of guidelines and controls [10], and the framework COBIT 5 [2] together with ITIL [11], and BIS [12] standards are used as reference in this literature review. Consequently, we mainly aimed at identifying mappings and mapping procedures that consider at least one of these standards.

Inclusion Criteria
• Deals with mapping of requirements or controls between different security standards • Contains mapping tables or documents tools to (semi-) automate the creation of mapping tables • Looks at standards mappings with at least one of the following standards and guidelines: BSI, COBIT, ISO/IEC 27001 (or 27002), ITIL, NIST SP-800, PCI-DSS • Or: looks at standards-agnostic mapping techniques

Exclusion Criteria
• References obsolete standards • Is not fully available • Is written in a language other than English or German

https://doi.org/10.30844/wi_2020_l4-mussmann

• Published before 2004

To find relevant scientific literature, ACM Digital Library, SpringerLink, IEEEXplore, and ScienceDirect were used as the primary search engines, dblp [13] as the backup search engine. Since this literature review is multivocal, DART-Europe [14] and Google [15] were used to find grey literature and other material pertinent to standards mapping strategies. The journals Computer Standards & Interfaces, International Journal of Standardization Research, and the Journal of Computer Science were identified as additional sources for potentially relevant articles. The table of contents of these journals were reviewed manually for relevant articles according to the inclusion and exclusion criteria listed in Table 1.

The search string building blocks used in the systematic literature review were *information security, cyber security, privacy, standard, framework, best practice, mapping, compar*,* and *harmoni*.* In a pilot search, the term *best practice* was found to be generally used synonymously with the term *standard* and thus included in the set. Furthermore, we added the search term *privacy* to find mappings between security standards and the GDPR. The term *requirement* was used in the pilot study but did not improve the results and was subsequently dropped.

Combining these building blocks lead to the search string that was used with all search engines during the literature search as shown in Table 2. Resources were included based on the inclusion and exclusion criteria listed in Table 1.

Table 1. Inclusion and Exclusion Criteria

Table 2. Systematic Literature Review, Search Process for Scientific Publications

IEEEXplore	*Search Mode: title, abstract, metadata*	**1,980 Results**
(“Information security” OR “cyber security” OR “privacy”) AND (standard OR framework OR “best practice”) AND (mapping OR compar* OR harm*)		
ACM Digital Library	*Search Mode: full text*	**756 Results**
+(“inforamtion security” “cyber security” “privacy”)+(standard framework “best practice”) +(mapping comparing comparison harmonizing)		
Springer Link	*Search Mode: full text, specific sections only*+	**1,501 Results**
(“information security” OR “cyber security” OR “privacy”) AND (standard OR framework OR “best practice” AND (mapping OR compar OR harmon)		
Science Direct	*Search Mode: title, abstract, keyword*	**88 Results**
(“information security” OR “cyber security”) AND (standards OR frameworks) AND (mapping OR comparison OR comparing OR harominzation OR comparison OR comparing OR harmonization OR harmonizing)		
dblp	*Search Mode: title, metadata*	**22 Results**
(security standard | standard) (map| harmoni | compar)		

+) Appropriate sub-disciplines from sections “IT in Business” and “Computer Science” were chosen to ensure a manageable result set. A full-text search (the only search option available) over all disciplines would have returned over 30,000 publications – mostly publications irrelevant to this literature review.

https://doi.org/10.30844/wi_2020_l4-mussmann

A preliminary search did not return any relevant results prior 2004 that did not violate any inclusion or triggered any exclusion criteria. Therefore, we added another exclusion criterion for resources published before 2004.

Figure 1 illustrates the overall search process. After identifying potential resources and removing duplicates, a screening step was conducted where each of the two main authors of this study processed roughly half of the identified articles. This consisted of scanning title and abstract to remove irrelevant publications from the result set. This step was necessary because the search terms for this literature review are ambiguous and lead to a great number of false positives (e.g. mapping studies, papers on the research and development of standards).

If a decision to include or exclude a resource could not be made based on title and abstract, the introduction and conclusion were taken into consideration and a second researcher was involved in the screening process. If no immediate agreement could be reached, the articles in question were kept in the pool of potential matches for the quality assessment stage.

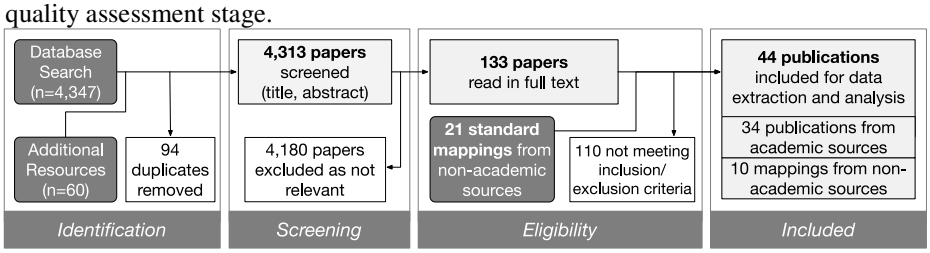

Figure 1. Search Process

The next stage of the selection process involved a thorough assessment of the articles' content and quality. The applied quality criteria differed depending on the actual contribution and type of each article. If an article described a methodology to create standards mappings, it was primarily assessed regarding its soundness, completeness and achieved result quality. If a mapping between security standards was the main contribution of an article, it was primarily assessed regarding the completeness and correctness of the mapping. Standards mappings from non-academic resources were excluded if they did not create new mappings (i.e. were a duplicate of mappings offered by standards or government organisations), used outdated sources or were not publicly available. This step was performed in parallel by the two main authors of this study on all articles and mappings in the set of potential matches. Each paper was subsequently discussed until the researchers agreed on whether to keep the article for the data extraction, synthesis and analysis concluded this step.

The systematic literature review was conducted in February 2019 in accordance with the previously described process and returned 44 relevant resources, 34 of which are academic publication and 10 mappings from non-academic sources. To ensure the completeness of the identified resources, we performed one snowballing iteration [16]. We used the identified resources as start set and performed a backward (finding resources cited by resource x of the start set) and a forward snowballing (finding

https://doi.org/10.30844/wi_2020_l4-mussmann

resources citing resource x of the start set) iteration. We did not identify suitable new resources in the snowballing iteration and could therefore conclude that our set of identified resources was complete.

From the 44 identified resources, general and more specific information was extracted. Each resource was given an ID, and the assessment date, a brief justification of why the resource was accepted in the literature review (based on the inclusion and exclusion criteria), and a quality assessment. Bibliographical information and the DOI reference were extracted from the resource. If the resource dealt with specific standards, these standards were extracted and the resource annotated with the number of standards, their names and relevant standards organisations. From research papers, methodology of the study, findings and conclusions were additionally obtained. Finally, a short summary of each scientific publication's main contribution, methods and ideas was produced for later reference.

Data synthesis was performed using quantitative techniques (descriptive statistics and meta-analysis). The 44 publications were then further assessed in a qualitative manner by means of a thematic analysis [17] to systematically derive answers to our research questions. We present these findings in Section 3.

3 Results and Discussion

In general, we could observe that most of the scientific publication did not present actionable security standards mappings but focused on the presentation of their respective methodology. Mappings between standards were either shown for subsets of

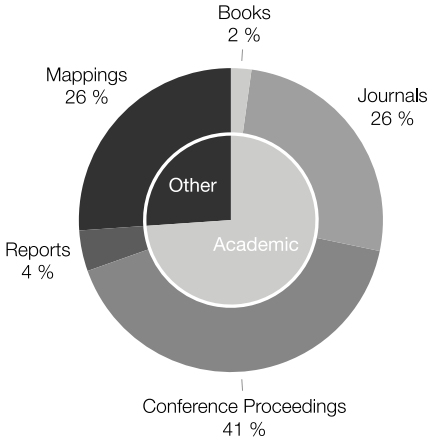

Figure 2. Selected Publication Sources

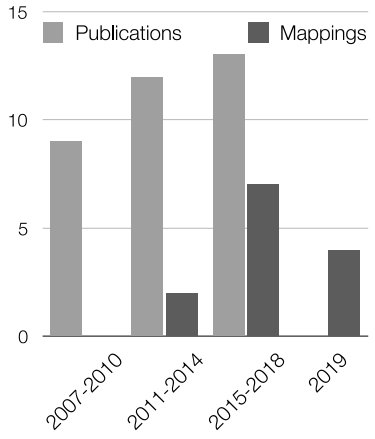

Figure 3. Publication Years

standard controls or on an abstract level (e.g. mapping terms and definitions between standards). Complete mapping tables were only available from non-academic sources

https://doi.org/10.30844/wi_2020_l4-mussmann

such as standard organisations or common interest groups. Figure 2 shows the statistics of selected publication categories and Figure 3 the distribution of the selected publications by year (grouped in three-year timespans). The lack of identified scientific publications in 2019 is due to the timeframe of our study.

We could observe a slight positive trend in publication interest from the scientific community in security standards mappings. We attribute the increase of scientific publications over the investigated timespan mainly to two events: The ISO 27001 standard update in 2013 and the EU GDPR coming into effect in 2018.

Table 4 gives an overview of the information extracted from the research papers. 19 papers propose standards mapping approaches using ontologies, 12 introduce manual comparison methods, and two use natural language processing (NLP). Two papers are concerned with automating the harmonisation process as much as possible, while seven papers detail frameworks for semi-automatic harmonisation efforts. The majority of papers use at least two standards to illustrate their proposed methodology. Six papers map one standard to standardized ontologies or models respectively and one paper creates a standards-agnostic ontology. ISO/IEC 27k standards are used most often, followed by COBIT, ITIL, and the BSI Baseline Protection methodology.

3.1 Security Standards Mappings

The mappings created and published by researchers are done either on selected parts of the standards only or on a higher level (such as mapping general goals and concepts of standards to each other). This can, at best, be a starting point for an in-depth standards mapping. There may be such in-depth mappings created by researchers, but this systematic literature review did not find a paper with an exhaustive standards mapping.

Table 3. Security Standards Mapping Tables

Organisation	*Standards*
BSI (G) [18]	ISO 27001:2013, BSI Grundschutz
CISA (S) [19]	PCI-DSS, ISO/IEC 27001
CSA (S) [20]	COBIT 5, ISO/IEC 27k, NIST SP800-53, PCI-DSS, …
ENISA (S) [21]	ISF Standard 2007, COBIT, ISO/IEC 24762:2008
Michael Falk (I) [22]	ISO 27001:2005, COBIT 4.1, ISO 20000-1
HHS (G) [23]	HIPAA, COBIT 5, ISO/IEC 27001:2013, NIST SP800-53
OneTrust C [24]	ISO 27001, GDPR
InformationShield (C) [25]	PCI-DSS v3, ISO 27002
ISACA (S) [26]	ISO/IEC 27001, COBIT 4.1
ISO27001security (C) [27]	GDPR, ISO27k
I: Individual C: Company	G: Government Organisation S: Standards Organisation

Table 3 lists the mapping tables we found in the literature study. They have been published either by individual experts (I), companies (C), standards organisations (S) or government organisations (G). Standards organisations are organisations that create

https://doi.org/10.30844/wi_2020_l4-mussmann

and maintain technical standards, potentially operate internationally and are not part of a national government. Government organisations, too, create and maintain standards but are part of a national government (e.g. HHS: United States Department of Health and Human Services). Companies publishing standards mappings are often consulting or software companies (such as IsecT, owner of iso27001security) that offer free access to part of their standards mappings product range.

The mapping tables found (see Table 3) were mostly created by standards organisations, for example, ENISA, ISACA, or CSA, companies such as OneTrust, or government organisations. ISACA offers mappings such as [26], a mapping of COBIT to ISO 27001. The mapping by ENISA [21] maps three security standards at once: ISO 24762, COBIT, and ISF, and the mapping by CISA [19] compares PCI-DSS to ISO 27001. The ISO 27001 is mapped often and against very different standards, as well as frameworks such as HIPAA or the GDPR.

The Cloud Controls Matrix of the Cloud Security Alliance [20] is the largest mapping table found in this literature review. It is a mapping table for standards and regulatory documents pertinent to cloud computing providers. It maps relevant sections of 41 different standards and regulatory documents to cloud controls. Based on this matrix it can be argued that there exist partial mappings for these 41 standards and regulations. The most prominent standards the Cloud Controls Matrix maps are the ISO 27k standards, COBIT, ITIL, PCI-DSS and NIST SP800-53.

Fully available mapping tables most frequently map the ISO 27k standards to NIST SP800-53 [10], COBIT [22, 26], and the GDPR [27]. Scientific publications use a wider range of standards and regulations and also map ISO 27k to ITIL [28], ISSA 51343 and NISTIR 7621 [29], BSI Grundschutz [30, 31], or regulations such as FISMA and HIPAA [32].

Standards organisations and companies focus on mapping ISO 27k and COBIT, and government organisations provide mappings for these standards with regulatory frameworks such as HIPAA, GDPR, or FISMA. Scientific research is less focused on the immediate value of mappings or mapping strategies and thus compares a greater range of standards and regulations. However, a focus on ISO 27k standards can be identified in scientific publications as well.

3.2 Creation of Security Standards Mappings

Of the scientific papers found in this systematic literature review, 13 out of 34 propose manual mapping strategies. As far as could be determined, all the mappings available from standards organisations, companies, and government organisations listed in Table 3 are created manually.

Of the papers listed in Table 4, Breaux et al. [33] and Ridley et al. [34] apply pre-existing methods from research unrelated to security standards mapping to create systematic mapping strategies. Beckers et al. [30], while still basing their mapping strategy on previous research, develop a more extensive manual mapping strategy specifically for security standards mapping. Mapping strategies themselves play a subordinate role in the papers of Di Giulio [31, 35, 36] and Gikas [32].

https://doi.org/10.30844/wi_2020_l4-mussmann

Overall, it seems that manual mapping strategies are regarded as the simplest and most accessible method to apply when focusing on directly comparing standards – as is evident from the standards organisations that all seem to create mapping tables manually, for example the Cloud Controls Matrix [37], and research papers such as the works of Di Giulio [31, 35, 36]. The methodology detailed for these mappings is simple (a three-step analysis [31, 35, 36], four main instructions to conduct the mapping process [37]) and therefore necessarily open to interpretation. When more elaborate frameworks for manual standard comparisons are used (e.g., Breaux et al. [33], Ridley et al. [34]) the frameworks are created in isolation without discussing other research and security standards mapping strategies or methodologies. Beckers et al. [30] are the exception. They base their methodology on previous research by Sunyaev [38] and others.

Nineteen of the papers in Table 4 research mapping strategies based on security ontologies. Security ontology research itself is a much larger field with publications such as Fenz et al. [39], Herzog et al. [40] and many more. An overview of some of the existing security ontologies is presented in Souag et al. [41]. There is a lot more continuity in strategies using security ontologies compared to manual mapping strategies. This is partly due to the underlying methodology, partly due to some ontologies being generally known, such as ontologies by Fenz et al. [39, 42]. Ramanauskaite et al. [29], analyse existing ontologies from Fenz et al. [39, 42] and others to create an improved security ontology for security standards.

Research into security ontologies to map standards is regarded as necessary to create unambiguous, systematic, and at least semi-automatic mapping strategies. Research papers such as Beckers et al. [30] (manual mapping strategy), Bartolini et al. [43] (NLP-

https://doi.org/10.30844/wi_2020_l4-mussmann

Table 4. Standard Mapping Procedures

Author(s)	*No Stds.*	*Standards*	*Methodology*				*Automation*			
			Ontology	*Manual*	*NLP*	*Other*	*None*	*Tool*	*Semi*	*Automatic*
Abdullah et al. [44]	-	Agnostic	✓				✓			
Almeida et al. [45, 46]	3	COBIT 5, ITIL, ISO 27001	✓					✓		
Bartolini et al. [43]	2	GDPR, ISO 27001			✓				✓	
Beckers et al. [30, 47]	3	CC, BSI, ISO 27001		✓			✓			
Breaux et al. [33]	3	NIST SP800-53, ISO 27002, CCM		✓			✓			
CSA [37]	>6	COBIT 5, ISO 27001, BSI, …		✓			✓			
Cheng&Lim-Cheng [48]	3	COBIT 5, ISO 27002, PCI-DSS v3	✓						✓	
Di Giulio et al. [31, 25, 26]	4	ISO 27001, BIS C5, Fed RAMP, …		✓			✓			
Ekelhart et al. [49]	1	CC	✓					✓		
Fenz et al. [42,50-52]	1	BSI, ISO 27001, ISO 27001	✓						✓	
Gikas [32]	4	HIPAA, ISO 27000, PCI-DSS, …		✓			✓			
Haufe et al. [5]	3	ISO 27001, COBIT, ITIL		✓			✓			
Hulitt&Rayford[53]	2	FISMA, FIPS				✓			✓	
Koelle et al. [54]	>6	Misc				✓				✓
Nicho [55]	2	COBIT, PCI-DSS		✓			✓	✓		
Pardo et al. [56-59]	>6	ISO 27001, 27002, COBIT, ITIL, …	✓	✓			✓	✓		
Pardo et al. [28, 60, 61]	>6	COBIT 4.1, Basel II, VAL IT, …	✓							
Pardo et al. [62]	6	ISO 27001, ISO 20000-2	✓							
Ramanauskaite et al. [29, 63]	4	ISO 27001, PCI-DSS, BSI, …	✓				✓	✓		
Ridley et al. [34]	2	COBIT, ACSI 33		✓			✓			
Vorobiev et al. [64]	>6	Misc ISO standards	✓				✓			
Winter et al. [65]	3	ISO 27000, 27001, ISO 34011			✓					✓

https://doi.org/10.30844/wi_2020_l4-mussmann

based semi-automated mapping framework), and Koelle et al. [54] (automated mapping methodology), too, use a common terminology in their respective frameworks.

There exist mappings of different standards to security ontologies, for example ISO 27001 [42], PCD-ISS [29], COBIT [2], and ITIL [28], and standards organisations such as NIST offer drafts [66] and software [67] to do with ontologies.

3.3 Natural Language Processing

While the literature review found manual standard mapping methodologies and several different security ontologies to use for security standards mapping, no paper found proposed a technique based on natural language processing (NLP) and machine learning (ML). The powerful ML techniques of deep learning, already well established in other areas, seem of no relevance to researchers looking into standards mapping. This is even more surprising when considering that research into harmonising laws and regulations – arguably very similar to harmonising security standards – uses NLP approaches as, for example, in [68], [69], and [70].

There are, however, two papers listed in Table 4 that use NLP to (semi-) automate the standards and regulations comparison process authored by Winter et al. [65] and Bartolini et al. [43]. These two papers were found using the Google search engine and search terms explicitly containing *natural language processing* or *NLP*. Both papers come from the legal and regulatory domain and focus on compliance and the creation of tools to support organisations in the compliance process. Their tool-supported approach is very different from all the other approaches detailed above. Both create frameworks that compare aspects of regulations and standards with each other and use the framework to implement either a tool to support the user in compliance management [43], or a tool to completely automate the extraction and comparison process [65]. Neither of the tools can be considered mature, but the fact that their work goes beyond providing mainly visual clues for harmonisation/comparison of security standards sets these papers apart from the rest – and would do so even without the use of NLP techniques.

3.4 Limitations

The presented literature review deviated from Kitchenham's best-practice guidelines [7], most prominently with the inclusion of grey literature sources. This, arguably, poses a potential threat to the construct validity of our work. We proactively addressed this potential issue by additionally following the guidelines for multivocal literature reviews by Garousi et al. [8]. While the process for identifying primary studies from scientific sources was thoroughly conducted and documented, we might have missed potential sources from non-academic sources by restricting ourselves to a mostly manual search of governmental and standard organisations offerings. This limits the external validity of the presented research endeavor.

https://doi.org/10.30844/wi_2020_l4-mussmann

4 Conclusion

Current research in security standards mapping methodology is limited. Although there are scientific publications on mapping strategies available as well as a quite extensive research into creating ontologies for information security, it seems like this is a field where more research should be happening considering the importance of security standards today.

Standards mappings, while discussed in scientific research, usually are executed outside of academia. The mix of standards organisations, governments, and security companies that create and distribute security mappings was unexpected, as was the relative dearth of available security standards mappings. However, there are many companies (e.g. [71, 72]) that sell generic standards mappings (e.g. mapping ISO 27001 [71, 72], COBIT [71, 72], etc.) and offer tool-support for companies to create bespoken standard mapping tables.

It is surprising that during this systematic literature review, no research explicitly considering the creation of standards mappings using NLP was found. These two identified resources focus strictly on compliance and harmonisation of regulations with standards. The frameworks these publications describe, however, could potentially be extended to support security standards mapping as well. In general, (full) automatisation of the mapping process, while acknowledged as desirable, is not the primary focus of scientific research endeavors identified in this systematic literature review.

We propose that future research in security standard mappings should incorporate NLP techniques, maybe in conjunction with existing security ontologies. This could yield promising results and considerably simplify the security standards mapping process, or any standards mapping process, for stakeholders. Such research is, in a similar fashion as described in [43, 65], already being done in the legal domain. Future research should additionally consider these existing methodologies and investigate whether they can be modified to fit security standards mapping requirements or at least serve as a building block for a more efficient and potentially automatic creation of information security standards mappings.

5 Acknowledgements

This work has been partially sponsored by the Austrian Federal Ministry of Education, Science and Research by FFG Project 855383 SALSA “Living Safety&Security Cases for Cyber-Physical Systems Certification” (Funding program “ICT of the Future”).

References

1. Purser, S.: Standards for Cyber Security. In: Hathaway, M.E. (ed.): Best Practices in Computer Network Defense: Incident Detection and Response. IOS Press (2014)

https://doi.org/10.30844/wi_2020_l4-mussmann

2. ISACA. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISA (2012)
3. International Organisation for Standardization. ISO/IEC 27001: Information technology - Security techniques - Information security management system - Requirements. Standard (2013)
4. PCI Security Standards Council. PCI DSS v3.2.1. Standard. https://www.pcisecuritystandards.org/document_librarycategory=pcidss&document=pci_dss. (Accessed: 28.01.2019)
5. Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., Stantchev, V.: Security Management Standards: A Mapping. In: Procedia Computer Science, vol. 100 pp. 755-761. Elsevier Online (2016)
6. Olifer, D.: Evaluation Metrics for Ontology-Based Security Standards Mapping. In: 2015 Open Conference of Electrical, Electronic and Information Sciences (eStream). IEEE (2015)
7. Kitchenham, B.: Procedures for Performing Systematic Reviews. In: Keele University, vol. 33, pp. 1–26. Keele, UK (2004)
8. Garousi, V., Felderer, M., Mäntylä, M.V.: The Need for Multivocal Literature Reviews in Software Engineering: Complementing Systematic Literature Reviews with Grey Literature. In: Proceedings of the 20th Intern. Conf. on Evaluation and Assessment in Software Engineering (EASE '16), p. 26:1-26:6. ACM, New York (2016)
9. Hulsebosch, B.: White paper: Inventory and Classification of Cyber Security Standards. Independent Summary of the Final Report. Technical Report (2015)
10. National Institute of Standards and Technology.: NIST Special Publication 800-53 Information Security. CreateSpace, Paramount (2013)
11. Axelos.: ITIL – Service Lifecycle Publication Suite. The Stationery Office, London (2011)
12. Bundesamt für Sicherheit in der Informationstechnik. BSI IT-Grundschutz-Kompendium – Edition 2018. Standard (2018)
13. The dblp Team: dblp Computer Science Bibliography. Monthly Snapshot release of February 2019. https://dbl.org/xml/release/dblp-2019-02-01.xml.gz (2019)
14. LIBER: The DART-Europe E-theses Portal. https://www.dart-europe.eu (Accessed 10.02.2019)
15. Google Inc: Google Search https://www.google.com (Accessed: 12.02.2019)
16. Wohlin, C.: Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering. In: Proceedings of the 18th Intern. Conf. on Evaluation and Assessment in Software Engineering, pp. 321–330. Citeseer, ACM, New York (2014)
17. Guest, G., MacQueen, K.M., Namey, E.E.: Applied thematic analysis. Sage Publications, Los Angeles (2012)
18. Bundesamt für Sicherheit in der Informationstechnik. Zuordnungstabelle ISO zum modernisierten IT-Grundschutz. Technical Report, BSI (2018)
19. Mataracioglu, T.. 2016. Comparison of PCI Dss and ISO/IEC 27001 Standards. In: ISACA Journal, 2016 vol. 1. Online (2016)
20. Cloud Security Alliance. Cloud Controls Matrix. Standard (2018)
21. ENISA. Metaframework. Technical Report (2011)
22. Falk, M.: Ableitung des Control-Frameworks für IT-Compliance. In: IT-Compliance in der Corporate Governance, pp. 149–246. Gabler Verlag, Wiesbaden (2012)
23. DHHS Office for Civil Rights. HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework. Technical Report. U.S. Department of Health & Human Services (2016)

https://doi.org/10.30844/wi_2020_l4-mussmann

24. Trevor, H.J., Kabir, B.: Bridging ISO 27001 to GDPR: Where Security and Privacy Share Common Ground. Technical Report. IAPP-OneTrust Research. (2018)
25. InformationShield. PCI-DSS Policy Mapping Table. Mapping.
26. Oparaugo, C.: ISO/IEC 27001 Process Mapping to COBIT 4.1 to Derive a Balanced Scorecard for IT Governance. COBIT Focus. Online (2015)
27. ISO27001Security: Mapping Between GDPR (the EU General Data Protection Regulation) and ISO27k. Technical Report (2016)
28. Pardo, C., Pino, F.J., García, F., Piattini, M., Baldassarre, M.T.: An Ontology for the Harmonization of Multiple Standards and Models. In: Computer Standards & Interfaces, vol. 34, no. 1, pp. 48-59. Elsevier, Online (2012)
29. Ramanauskaite, S., Olifer, D., Goranin, N., Cenys, A.: Security Ontology for Adaptive Mapping of Security Standards. Intern. Journal of Computers, Communications & Control (IJCCC), vol. 8, no. 6, pp. 878-890. CCC Publications, Online (2013)
30. Beckers, K., Côté, I., Fenz, S., Hatebur, D., Heisel, M.: A Structured Comparison of Security Standards. In: Engineering Secure Future Internet Services and Systems, pp. 1–34. Springer, Heidelberg (2014)
31. Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R., Bashir, M.N.: IT Security and Privacy Standards in Comparison: Improving FedRAMP Authorization for Cloud Service Providers. In 2017 17th IEEE ACM Intern. Symposium on Cluster, Cloud and Grid Computing (CCGRID), pp. 1090–1099. IEEE (2017)
32. Gikas,C.: 2010. A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. In: Information Security Journal: A Global Perspective, vol. 19, no. 3, pp. 132-141. Taylor & Francis, Online (2010)
33. Breaux, T.D., Gordon, D.G., Papanikolaou, N., Pearson, S.: Mapping Legal Requirements to IT Controls. In: 6th Intern. Workshop on Req. Eng. and Law, 11–20. IEEE (2013)
34. Ridley, G., Hartnett, J., Jarern-Imakul, W.: Mapping Information Security Standards: A Counter-Terrorism Example. In: ECIS 2008 proceedings, pp. 1370–1381. (2008)
35. Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R.H., Bashir, M.N.: Cloud security certifications: a comparison to improve cloud service provider security. In: Proceedings of the Second Intern. Conf. on IoT and Cloud Comp. ACM, New York (2017)
36. Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R.H., Bashir, M.N.: Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security? In: 2017 IEEE 10th Intern. Conf. on Cloud Computing (CLOUD), pp. 50–57. IEEE (2017)
37. Catteddu, D., Chin, V., Cordero, S., Foo, A.P., Laris, K., Maaloul, A., Pannetrat, A., Roza, M., Savanovic, D., Skoutaris, E., Tierling, E.: Methodology for the Mapping of the Cloud Controls Matrix (CCM). Technical Report (2018)
38. Sunyaev, A.: Health-Care Telematics in Germany: Design and Application of a Security Analysis Method. Springer, Heidelberg, Germany (2011)
39. Fenz, S., Ekelhart, A.: Formalizing Information Security Knowledge. In: Proceedings of the 4th Intern. Symposium on Information, Computer, and Communications Security, pp. 183-194. ACM, New York (2009)
40. Herzog, A., Shahmehri, N., Duma, C.: An Ontology of Information Security. In: Intern. Journal of Information Security and Privacy (IJISP), vol. 1, no. 4, pp. 1-23. IGI Publishing, Hershey (2007)
41. Souag, A., Salinesi, C., Comyn-Wattiau, I.: Ontologies for Security Requirements: A Literature Survey and classification. In: Intern. Conf. on Advanced Information Systems Engineering, pp. 61–69. Springer, Berlin, Heidelberg, Germany (2012)
42. Fenz, S., Goluch, G., Ekelhart, A., Riedl, B., Weippl, E.: Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard. In: 13th Pacific

https://doi.org/10.30844/wi_2020_l4-mussmann

Rim Intern. Symposium on Dependable Computing (PRDC 2007), pp. 381-388. IEEE (2007)
43. Bartolini, C., Giurgiu, A., Lenzini, G., Robaldo, L.: A Framework to Reason about the Legal Compliance of Security Standards. In: Tenth Intern. Workshop on Juris-informatics (JURISIN). (2016)
44. Abdullah, N.S., Indulska, M., Sadiq, S.: Compliance Management Ontology — a Shared Conceptualization for Research and Practice in Compliance Management. In: Information Systems Frontiers, vol. 18, no. 5, pp. 995–1020. Springer, Heidelberg (2016)
45. Almeida, R., Lourinho, R., Mira da Silva, M., Pereira, R.: A Model for Assessing COBIT 5 and ISO 27001 Simultaneously. In: 2018 IEEE 20th Conference on Business Informatics (CBI), vol. 1, pp. 60–69. IEEE (2018)
46. Almeida, R., Pinto, P., Mira da Silva, M.: Using ArchiMate to assess COBIT 5 and ITIL implementations. In: 25th Intern. Conf. on Information Systems Development, pp. 235–246. Katowice, Poland: University of Economics in Katowice (2016)
47. Beckers, K., Heiselm M., Solhaug, B., Stølen, K.: ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System. In: Engineering Secure Future Internet Services and Systems, pp. 315-344. Springer, Heidelberg (2014)
48. Cheng, D.C., Lim-Cheng, N.R.: An ontology-based framework to support multi-standard compliance for an enterprise. In: 2017 Intern. Conf. on Research and Innovation in Information Systems (ICRIIS), pp. 1–6. IEEE (2017)
49. Ecklhart, A., Fenz, S., Goluch, G., Weippl, E.: Ontological mapping of common criteria's security assurance requirements. In: IFIP Intern. Inf. Sec. Conf., pp. 85–95. Springer, Heidelberg (2007)
50. Fenz, S., Neubauer, T.: Ontology-based information security compliance determination and control selection on the example of ISO 27002. In: Information & Computer Security, vol. 26, no. 5, pp. 551-567. Emerald Insight, Online (2018)
51. Fenz, S., Plieschnegger, S., Hobel, H.: Mapping information security standard ISO 27002 to an ontological structure. In: Information & Computer Security, vol.24, no. 5, pp. 452-473. Emerald Insight, Online (2016)
52. Fenz, S., Pruckner, T., Manutscheri, A.: Ontological mapping of information security best-practice guidelines. In: International Conference on Business Information Systems (BSI '09), pp. 49–60. Springer, Heidelberg (2009)
53. Hulitt, E., Vaughn, R.B.: Information system security compliance to FISMA standard: a quantitative measure. In: Telecommunication Systems, vol. 45, no. 2, pp. 139-152. Springer, Heidelberg (2010)
54. Koelle, R., Strijland, W., Roels, S.: Towards Harmonising the Legislative, Regulatory, and Standards-Based Framework for ATM Security: Developing a Software Support Tool. In: 2013 Intern. Conference on Availability, Reliability and Security, pp. 787-793. IEEE (2013)
55. Nicho, M.: Incorporating COBIT best practices in PCI DSS V2. 0 for Effective Compliance. ISACA Journal, 2012 vol. 1, p. 42. Online (2012)
56. Pardo, C., Pino, F., García, F., Romero, F., Piattini, M., Baldassarre, M.T.: HProcessTOOL: a support tool in the harmonization of multiple reference models. In: Intern. Conf. on Computational Science and Its Applications, pp. 370–382. Springer, Heidelberg (2011)
57. Pardo, C., Pino, F.J., García, F., Piattini, M., Baldassarre, M.T.: A process for driving the harmonization of models. In: Proceedings of the 11th Intern. Conf. on Product Focused Software, pp. 51–54. ACM, New York (2010)

https://doi.org/10.30844/wi_2020_l4-mussmann

58. Pardo, C., Pino, F.J., García, F., Piattini, M., Baldassarre, M.T., Lemus, S.: Homogenization, comparison and integration: a harmonizing strategy for the unification of multi-models in the banking sector. In: Intern. Conf. on Product Focused Software Process Improvement, pp. 59–72. Springer, Heidelberg (2011)
59. Pardo, C., Pino, F.J., García, F., Velthius, M.P., Baldassarre, M.T.: Trends in harmonization of multiple reference models. In: Intern. Conf. on Evaluation of Novel Approaches to Software Engineering, pp. 61–73. Springer, Heidelberg (2010)
60. Pardo-Calvache, C.J., García-Rubio, F.O., Piattini-Velthuis, M., Pino-Correa, F.J., Baldassarre, M.T.: A reference ontology for harmonizing process-reference models. In: Revista Facultad de Ingeniería Universidad de Antioquia, vol. 73, pp. 29-42. Online (2014)
61. Pardo-Calvache, C.J., Pino, F.J., Félix García, Baldassarre, M.T., Piattini, M.: From chaos to the systematic harmonization of multiple reference models: A harmonization framework applied in two case studies. In: Journal of Systems and Software, vol. 86, no. 1, pp. 125-143. Elsevier, Online (2013)
62. Pardo, C., Pino, F.J., Garcia, F.: Towards an Integrated Management System (IMS), harmonizing the ISO/IEC 27001 and ISO/IEC 20000-2 Standards. In: Intern. Journal of Software Engineering and Its Applications, vol. 10, no. 9, pp. 217-230. Online (2016)
63. Ramanauskaite, S., Goranin, N., Cenys, A., Olifer, D.: Ontology-Based Security Standards Mapping Optimization by the Means of Graph Theory. In: Intern. congress on engineering and technology. (2013)
64. Vorobiev, V.I., Fedorchenko, L.N., Zabolotsky, V.P., and Lyubimov, A.V.: Ontology-based Analysis of Information Security Standards and Capabilities for their Harmonization. In: Proceedings of the 3rd Intern. Conf. on Sec. of Information and Networks, pp. 137–141. ACM, New York (2010)
65. Winter, K., Rinderle-Ma, S.: Detecting Constraints and their Relations from Regulatory Documents Using NLP Techniques. In: Panetto, H., Debruyne, C., Proper, H.A., Ardagna, C.A., Roman, D., Meersman, R. (eds.) OTM Confederated Intern. Conf. "On the Move to Meaningful Internet Systems", pp. 261–278. Springer, Heidelberg (2018)
66. Booth, H., Christopher. T.: NIST Draft: Vulnerability Description Ontology (VDO). Technical Report, NIST (2018)
67. Morris, K.C., Narayanan, A., Lechevalier, D.: NOVIS – NIST Ontological Visualisation. Technical Report (2017)
68. Papanikolaou, N.: Natural Language Processing of Rules and Regulations for Compliance in the Cloud. In: OTM Confederated Intern. Conf. "On the Move to Meaningful Internet Systems", pp. 620–627. Springer, Heidelberg (2012)
69. Cleland-Huang, J., Czauderna, A., Gibiec, M., Emenecker, J.: A Machine Learning Approach for Tracing Regulatory Codes to Product Specific Requirements. In: 2010 ACM/IEEE 32nd Intern. Conf. on Software Engineering, vol. 1, pp. 155–164. IEEE (2010)
70. Mandal. S., Gandhi, R., Siy, H.: Modular Norm Models: A Lightweight Approach for Modeling and Reasoning about Legal Compliance. In: 2017 IEEE DASC/PiCom/DataCom/CyberSciTech, pp. 657-662. IEEE (2017)
71. Allgress Inc: Mapping Subscription. https://allgress.com/compliance-mapping-subscription (Accessed 12.11.2019)
72. Advisera Expert Solutions Ltd. https//adviser.com (Accessed 12.11.2019)

https://doi.org/10.30844/wi_2020_l4-mussmann