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 Grundschutz 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 800-53[1] 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.

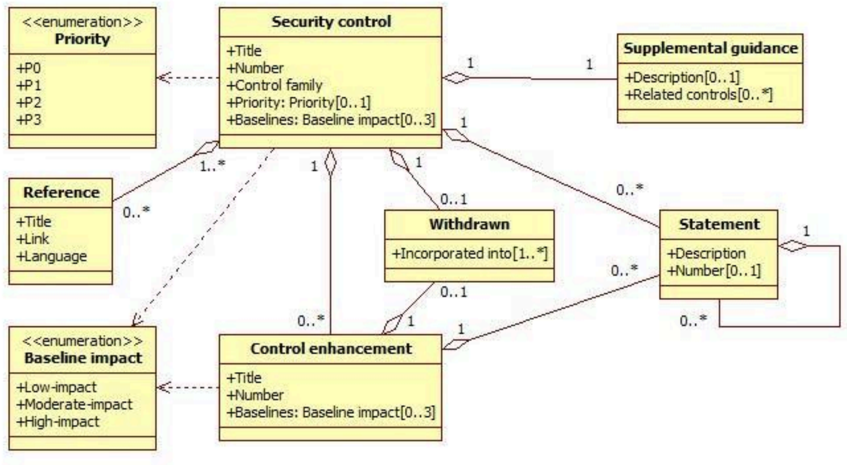


Fig 1. NIST SP 800-53 structural model.

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.

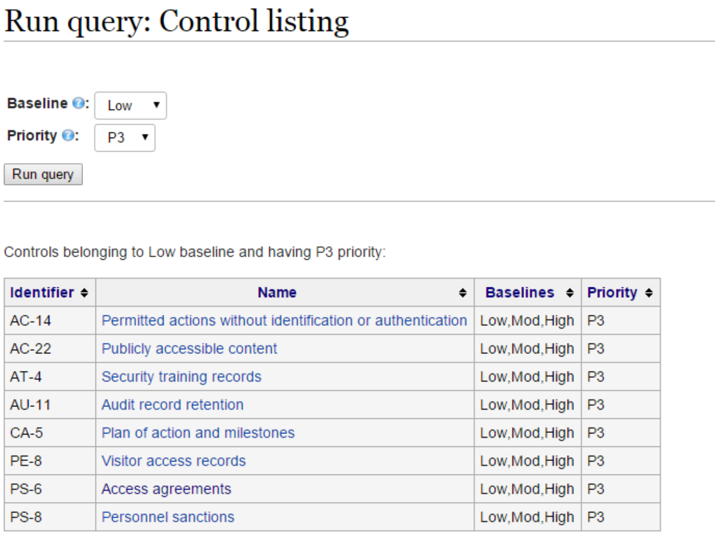
Validation of the constructed semantic model was performed in two ways. First, we used the SMW build-in special pages. The special pages provide metadata of the SMW contents such as list of all pages, pages with a property, and list of properties. Contents of the special pages were then validated against 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: Low

Priority: P3

Controls belonging to Low baseline and having P3 priority:

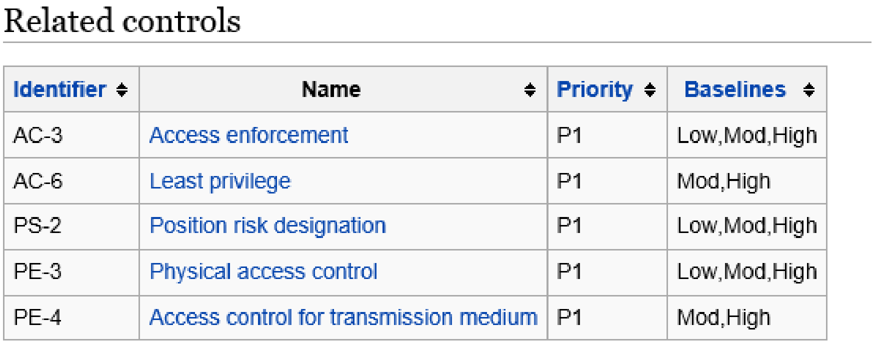
Identifier	Name	Baselines	Priority
AC-14	Permitted actions without identification or authentication	Low,Mod,High	P3
AC-22	Publicly accessible content	Low,Mod,High	P3
AT-4	Security training records	Low,Mod,High	P3
AU-11	Audit record retention	Low,Mod,High	P3
CA-5	Plan of action and milestones	Low,Mod,High	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

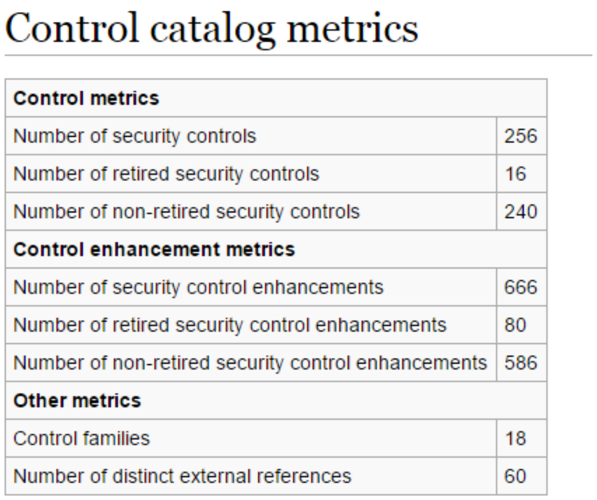
Identifier ♦	Name ♦	Priority ♦	Baselines ♦
AC-3	Access enforcement	P1	Low,Mod,High
AC-6	Least privilege	P1	Mod,High
PS-2	Position risk designation	P1	Low,Mod,High
PE-3	Physical access control	P1	Low,Mod,High
PE-4	Access control for transmission medium	P1	Mod,High

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.

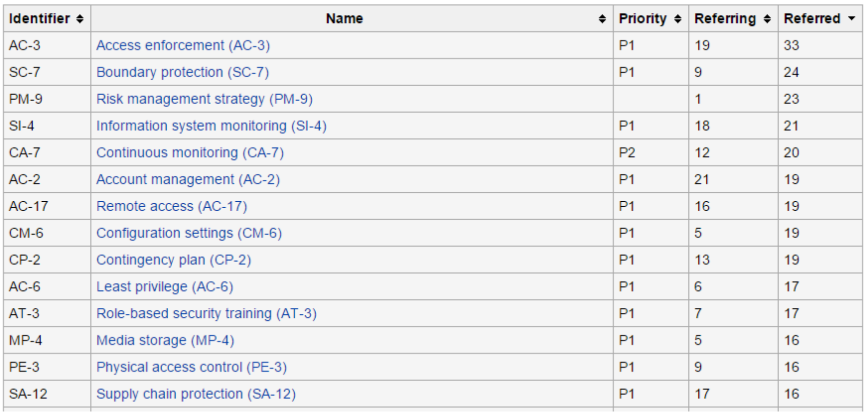


Control catalog metrics

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: PRIMIUM.

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.

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.