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.

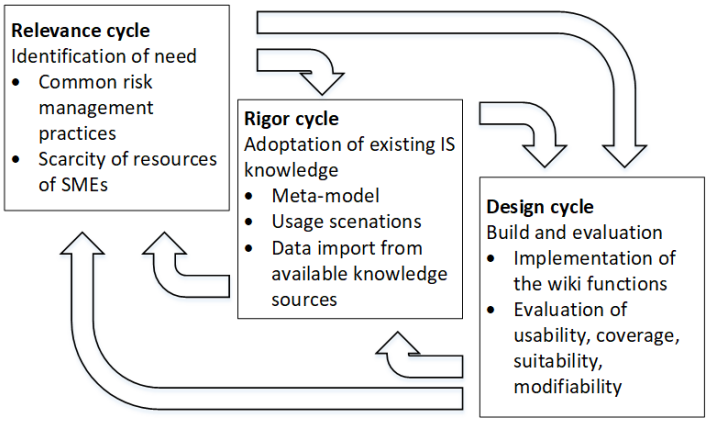

Fig. 1. Iterative design process presenting DSR cycles with outcomes of the cycles.

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.

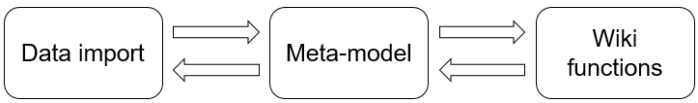

Fig. 2. Development cycles of the demonstrator.

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 Grundschutz 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.

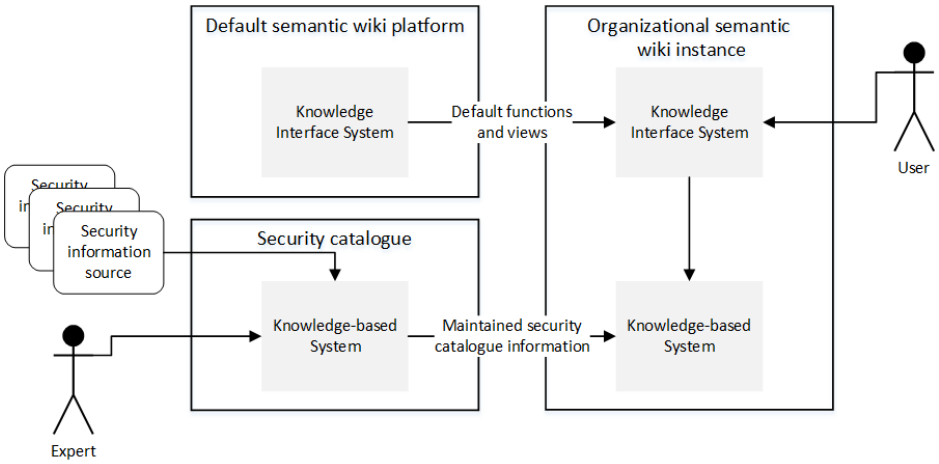

Fig. 3. Role of knowledge interface system and knowledge base.

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 argumented 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. Işik 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. Mejias 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.