Using Security Requirements Engineering Approaches to Support ISO 27001 Information Security Management Systems Development and Documentation

Kristian Beckers, Stephan Faßbender, Maritta Heisel
paluno - The Ruhr Institute for Software Technology – University of Duisburg-Essen, Germany
Email: {firstname.lastname}@uni-duisburg-essen.de

Holger Schmidt
ITESYS - Institut für technische Systeme GmbH, Germany
Email: h.schmidt@itesys.de

***Abstract*—An ISO 27001 compliant information security management system is difficult to create, due to the the limited support for system development and documentation provided in the standard.**

We present a structured analysis of the documentation and development requirements in the ISO 27001 standard. Moreover, we investigate to what extent existing security requirements engineering approaches fulfill these requirements. We developed relations between these approaches and the ISO 27001 standard using a conceptual framework originally developed for comparing security requirements engineering methods. The relations include comparisons of important terms, techniques, and documentation artifacts. In addition, we show practical applications of our results.

***Keywords*-security standards, requirements engineering, ISO27000, ISO27001, compliance, security**

I. Introduction

Aligning organizations to meet security demands is a challenging task. Security standards, e.g. the ISO 27000 series of standards offer a way to attain this goal. The normative standard of the aforementioned series, the ISO 27001, contains the requirements for an *Information Security Management System (ISMS)* [1]. The standard prescribes a process, which tailors security to the needs of any kind of organization. The remaining standards of the ISO 27000 series describe parts, or usage scenarios, of the ISMS in detail [2], [3]. For example, the ISO 27005 [4] describes information security risk management. The ISO 27005 has a certain significance as the ISO 27001 is risk-centered in many sections, and the ISO 27005 describes the risk assessment process and the risk documentation and management in detail. However, the ISO 27005 is not normative.

The ISMS consists of processes, procedures, and resources that can be software. Sparse descriptions in the standard are a problem during the establishment of an ISMS. For example, the required input for the *scope and boundaries* description is to consider "characteristics of the business, the organization, its location, assets and technology"[5, p. 4].

Moreover, the standard does not provide a method for assembling the necessary information or a pattern on *how to* structure that information.

Security requirements engineering (SRE) methods, on the other hand, provide structured elicitation and analysis of security requirements. [1] SRE methods can be part of the early phases of a given software development process. However, we propose not to limit SRE methods to software development. The structured elicitation and analysis of security requirements of SRE methods is also useful for different security engineering contexts. Therefore, we propose to use SRE methods to support security engineers in the development and documentation of an ISMS, compliant to ISO 27001. In addition, the ISMS is a process for security that may also rely on secure software. Thus, SRE methods can also support software engineers in building secure software for an ISMS.

Our work starts with a *top-down* approach. We systematically analyze the ISO 27001 standard in order to determine *where* and *how* SRE methods can support the development and documentation of an ISMS according to ISO 27001. First, we create a relation between the ISO 27001 standard and the conceptual framework (CF) of Fabian et al. [6]. Second, we use the relation of terminologies and notions from the CF to numerous SRE methods already provided by Fabian et al. Third, combining the relations of steps 1 and 2 we can relate the ISO 27001 with different SRE methods.

The second part of our work is a *bottom-up* approach. We support re-using documents created by an SRE method, so-called *SRE documents*. We can re-use the relation between the used SRE method and the CF to figure out *what* ISO 27001 section the SRE documents support. If this relation does not exist, we have to create it. It is sufficient to create a relation between the CF and the SRE method, because of the existing relation between the CF and ISO 27001. Thus, transitive relations from the ISO 27001 to existing SRE documents are possible.

The outcome of this analysis answers the research question, if and to what extent SRE approaches can support the development of an ISO 27001 compliant ISMS. Moreover, it answers the question in what way SRE methods provide

[1] In this paper we classify also security extensions of more general requirements engineering methods, e.g., Tropos and i* as SRE methods, because only SRE is the focus of this work.

the required documentation for an ISMS and how existing SRE documentation can be re-used for an ISMS.

The rest of the paper is organized as follows. Section II presents background on the ISO 27001 standard, and Sect. III presents the CF of Fabian et al. [6]. We set up a relation between the ISO 27001 standard and the CF in Sect. IV. In addition, we obtain a relation of security requirements methods to the ISO 27001. Sect. V discusses the practical application of our work, and Sect. **??** presents related work. Section VI concludes and gives directions for future research.

II. The ISO 27001 Standard

The ISO 27001 standard is structured according to the "Plan-Do-Check-Act" (PDCA) model, the so-called *ISO 27001 process* [5]. In the *Plan* phase an ISMS is established, in the *Do* phase the ISMS is implemented and operated, in the *Check* phase the ISMS is monitored and reviewed, and in the *Act* phase the ISMS is maintained and improved. In the *Plan* phase, the *scope and boundaries* of the ISMS, its *interested parties*, *environment*, *assets*, and all the *technology* involved are defined. In this phase, also the ISMS *policies*, *risk assessments*, *evaluations*, and *controls* are defined. Controls in the ISO 27001 are measures to *modify risk*. The ISO 27005 [4] refines this process for risk management and extends it with a pre-phase for information gathering.

The ISO 27001 standard demands a set of documents that describe the requirements for the ISMS. Moreover, certification of an ISMS according to the ISO 27001 standard is possible, based upon the documentation of the ISMS requirements.

III. A Conceptual Framework for Security Requirements Engineering

Notions and terminology differ in different SRE methods [6]. In order to be able to compare different SRE methods, Fabian et al. [6] developed a CF that explains and categorizes building blocks of SRE methods. In their survey the authors also use the CF to compare different SRE methods. Karpati et al. [7] conclude in their survey that the only existing "uniform conceptual framework for translations"of security terms and notions for SRE methods is the work of Fabian et al. [6]. Therefore, we use this CF and base our relations between the ISO 27001 and SRE methods on it. For simplicity's sake, we work on a subset of the CF. The CF considers security as a system property using the terminology of Michael Jackson [8], which defines that a *system* consists of a *machine* and its *environment*. The machine is the thing to be built, e.g., software. The part of the real world into which the machine will be integrated is the environment. The description of the desired behavior of the environment after the machine's integration is the so-called *requirement*. The CF considers four main building blocks of SRE methods: *Stakeholder Views*, *System Requirements*, *Specification and Domain Knowledge*, and *Threat Analysis*. **Stakeholder Views** identify and describe the stakeholders and their functional and non-functional goals and resulting functional and non-functional requirements. Stakeholders express security concerns via security goals. These goals are described towards an asset of the stakeholder, and they are refined into security requirements. **System Requirements** result from a reconciliation of all functional, security and other non-funtional requirements, while the stakeholder view perspective focuses on the requirements of one stakeholder in isolation. Hence, the system requirements analysis includes the elimination of conflicts between requirements and their prioritization. The result is a coherent set of system requirements. Requirements are properties the system has after the machine is built. The **Specification and Domain Knowledge** building block consists of *specifications*, *assumptions* and *facts*. The specification is the description of the interaction behavior of the machine with its environment. It is the basis for the construction of the machine. Assumptions and facts make up the *domain knowledge*. The domain knowledge describes the environment in which the machine will be integrated. In practical terms this means the security requirements have to be reviewed in context of the environment. The **Threat Analysis** focuses on *security properties* required by stakeholders. A violation of a security property is a potential loss for a stakeholder. This loss constitutes a risk for the stakeholder, which is reduced by countermeasures. A vulnerability may lead to a violation of a security property, and it is mitigated by a countermeasure.

Attacks actually exploit vulnerabilities, while threats only potentially exploit vulnerabilities. Attacks realize threats.

IV. Relating the ISO 27001 Standard and Security Requirements Engineering Methods

In the following, we present a matching between the ISO 27001 and SRE methods. First, we relate the terminologies of the ISO 27001 to the CF in Sect. IV-A. Second, we relate the building blocks of the CF to ISO 27001 sections in Sect. IV-B. Third, we present a relation between ISO sections 4.2.1 a, b and d and different SRE methods in Sects. IV-C, and IV-D. Three significant classes of SRE methods exist according to Fabian et al [6]: Goal-oriented, problem-related and risk-oriented SRE methods. We selected at least one kind of each class to show our mapping. We select KAOS and secure tropos for goal-oriented, SEPP for problem-oriented and CORAS for risk-oriented.

A. Relating the CF to ISO 27001 Terminology

Table I relates relevant terms for security from the CF by Fabian et al. [6] to the ISO 27001 standard. The matching benefits from the fact that both documents rely on ISO 13335 [9] definitions for several terms. we first relate the terms system, machine, and environment of the CF to the ISO 27001 standard. The system considered in the standard is

Table I: Correspondence between ISO 27001 terms and terms of the CF [6]

CF Fabian et al.	**ISO 27001**
System	The *organisation* is the "scope"of the standard [5, p. 1].
Machine	The *Information Security Management System (ISMS)* is the machine to be built [5, p. v].
Environment	The *scope and boundaries* of the "organization"[5, p. 4, Sec 4.2.1 a] relevant for the ISMS.
Security Goal	The standard uses *security objectives* [5, p. 4, Sec 4.2.1 b] instead of security goals.
Security Requirement	*Security requirement* is also used in ISO 27001 as a description of the "organization"after the "ISMS"is introduced [5, p. v,vi].
Specification	The ISMS's policy, controls, processes and procedures [5, p. vi] are the specification of the machine.
Stakeholder	The *Interested Parties* [5, p. vi] have security "expectations"that are input for the ISMS implementation as well as "security requirements".
Domain Knowledge	The *characteristics of the business, the organization, its location, assets and technology* [5, p. 4].
Availability	The definition in ISO/IEC 13335 [9] is also used [5, p. 2].
Confidentiality	The definition in ISO/IEC 13335 [9] is also used [5, p. 2].
Integrity	The definition in ISO/IEC 13335 [9] is also used [5, p. 2].
Asset	The definition in ISO/IEC 13335 [9] is also used [5, p. 2].
Threat	The definitions match. Threats are defined towards assets and threats exploit vulnerabilities [5, p. 4].
Vulnerability	The definitions match [5, p. 4].
Risk	The CF defines risk as "the potential loss of a stakeholder"[6, p. 13], while in ISO 27001 risk is not defined explicitly. However, the risk identification evolves around identifying asset, threat, vulnerability and the impact a loss of availability, confidentiality and availability has on an asset [5, p. 4]. Hence, we can conclude that the meaning is similar.

the organization, because it is the 'scope' of the standard [5, p. 1]. The machine to be build is the ISMS. The environment is equal to the scope and boundaries of the ISMS. The security goals are called security objectives in the standard, while the term security requirements has an equal meaning. The standard lists stakeholders as interested parties. The specification of the ISMS are its policies, controls, processes, and procedures. The domain knowledge in the standard is a description of the characteristics of the business. The definitions of the CIA triade, availability, confidentiality, and integrity, refer in both documents to the ISO 13335 [9] standard's definitions. The definition of assets, threats, vulnerabilities, and risks have similar definitions in both documents (see Table I). A detailed discussion can be found in [10].

B. Relating ISO 27001 Section 4 to SRE methods

ISO 27001 Section 4 describes the ISMS. Hence, we focus on this section in particular. Table III lists relations between subsections of ISO 27001 Section 4 and the CF's building blocks. We present all subsections of ISO 27001 Section 4.2, because these describe the establishment of the ISMS. In addition, we show risk management as a separate column, even though it is part of the CF's building block *threat analysis*. The reason is that some subsections of ISO 27001 Section 4 and SRE methods specifically focus on risk management. Moreover, the importance of risk in the ISO 27000 series of standards resulted in the standard ISO 27005 for information security risk management that specifies the risk management of the ISO 27001 [4]. A "+"in Tab. III marks a part of the section that can be supported by a building block of the CF. However, the free cells of the table do not imply that a method could not support that section of the ISO 27001. A *grey* row indicates that there are no explicit matches between the ISO 27001 section and the CF.

C. Relating ISO 27001 Sect. 4.2.1 a to SRE Methods

ISO 27001 Sec 4.2.1 a demands to "Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology, and including details of and justification for any exclusions from the scope."[5, p. 4].

The characteristics of the business includes *interested parties*, which are stakeholders in the CF terminology (see Tab. I) . The security expectations of the stakeholders are input for the ISMS [5, p. vi]. Moreover, ISO 27001 Sec 4.2.1 a states that assets shall be defined. The *Stakeholder Views* provide a description of stakeholders, their assets and security goals. In addition, the *characteristics of the business* are the functional and non-functional goals of the stakeholders Functional, non-functional, and security goals are

ISO 27001 Sec 4.2.1 a requires information about the location and technology of the organization. Furthermore, it requires information about *exclusions from the scope* of the ISMS. The *Specification and Domain Knowledge* contains

Table II: SRE methods supporting ISO 27001 Sect. 4.2.1 a

Methods	Stakeholder Views	Domain Knowledge
KAOS	x	x
Secure Tropos	x	
SEPP		x
CORAS		x

Table III: Relating ISO 27001 Section 4 to CF building block

Section	Description	SV	SR	SDK	TA
Sect. 4.1	General requirements	+	+	+	+
Sect. 4.2	Establish and manage the ISMS	+	+	+	+
Sect. 4.2.1	Establish the ISMS	+	+	+	+
Sect. 4.2.1 a	Define scope and boundaries	+			
Sect. 4.2.1 b	Define ISMS policy	+	+		+
Sect. 4.2.1 c	Define risk assessment				
Sect. 4.2.1 d	Identify the risk	+			+
Sect. 4.2.1 e	Analyse and evaluate risk			+	+
Sect. 4.2.1 f	Identify risk treatment				+
Sect. 4.2.1 g	Select controls				+
Sect. 4.2.1 h,i	Obtain management approval				
Sect. 4.2.1 j	Prepare a statement of applicability				+
Sect. 4.2.2	Implement and operate the ISMS				+
Sect. 4.2.3	Monitor and review the ISMS	+	+	+	+
Sect. 4.2.4	Maintain and improve the ISMS				
Sect. 4.3	Documentation requirements	+	+	+	+

SV(Stakeholder Views),**SR**(System Requirements), **SDK**(Specification and Domain Knowledge),**TA**(Threat Analysis)

information about the environment in the *Domain Knowledge*. This information includes location and technology of the organization. The information about the environment enables also decisions for *exclusions from the scope* of the ISMS.

This relation between ISO 27001 Sec 4.2.1 a and the CF's building blocks *Stakeholder Views* and *Specification and Domain Knowledge* provides in consequence a relation to SRE methods, because the work of Fabian et al. [6] already contains a relation between the CF and SRE methods. Table II shows the relation of several different SRE methods to the CF taken from [6]. The "x"in a field of the table means that there is a relation to a CF building block. However, the free cells of the table do not imply that a method could not support a section of the ISO 27001. Table II presents the goal-oriented SRE methods KAOS [11], [12] and Secure Tropos [13], [14], the problem-oriented method SEPP [15], and the risk analysis-based method CORAS [16].

KAOS' realization of the *Stakeholder Views* considers multiple stakeholders in and multiple views towards a system-to-be [6]. These views are different models of the system, e.g., *goal*, *object*, *agent*, and *security threat* models. Goals of stakeholders are modeled in a tree that refines the goals until a goal can be assigned to an agent. At this stage the goal becomes a requirement [6]. To sum up, KAOS describes the *organization* in the ISO 27001 standard via the views on it. It also realizes *Specification and Domain Knowledge*. The information about *assets*, *location*, and *technology* relevant for the ISO 27001 are included in different views.

Secure Tropos realizes *Stakeholder Views*. The method models actors and their goals. An actor in this method is also equivalent to a stakeholder [6]. Secure Tropos uses goals of stakeholders to model the *organization* in the ISO 27001 standard. Secure Tropos does not realize *Specification and Domain Knowledge*. The approach focuses on analyzing the trade-off relations between different security goals from stakeholders and their perspectives.

SEPP is a problem-based approach and does not realize *Stakeholder Views* explicitly. It centers around a description of the problem that the *machine* to be built shall solve. The problem is described in terms of the *environment* around it. SEPP realizes *Specification and Domain Knowledge* [6]. The method captures the domain knowledge in problem diagrams and natural language. This approach models the *environment* of the ISMS in a context diagram.

CORAS bases its data collection upon stakeholder interviews and investigations from risk experts. It generates a model from the resulting information. However, the interviews do not focus on the perspective of stakeholders, but solely on the target of the risk evaluation. CORAS realizes *Specification and Domain Knowledge*. The approach develops a model of the risk target, including assumptions about the target and its environment. The ISO 27001 description of the location, assets, and technologies are modeled as assumptions.

The ISO 27001 standard dictates a documentation that proves the relationship between chosen controls to the ISMS policies and objectives. This documentation has to contain a description of the *scope and boundaries* of the ISMS [5, p.13,Sec 4.3.1]. Therefore, the output of *Stakeholder Views* and *Specification and Domain Knowledge* of the different SRE methods in Tab. II supports the ISO 27001 documentation of the *scope and boundaries* of the ISMS.

D. Relating Section 4.2.1 d to SRE methods

ISO 27001 Sect. 4.2.1 d considers risk identification, which includes several typical elements of security require-

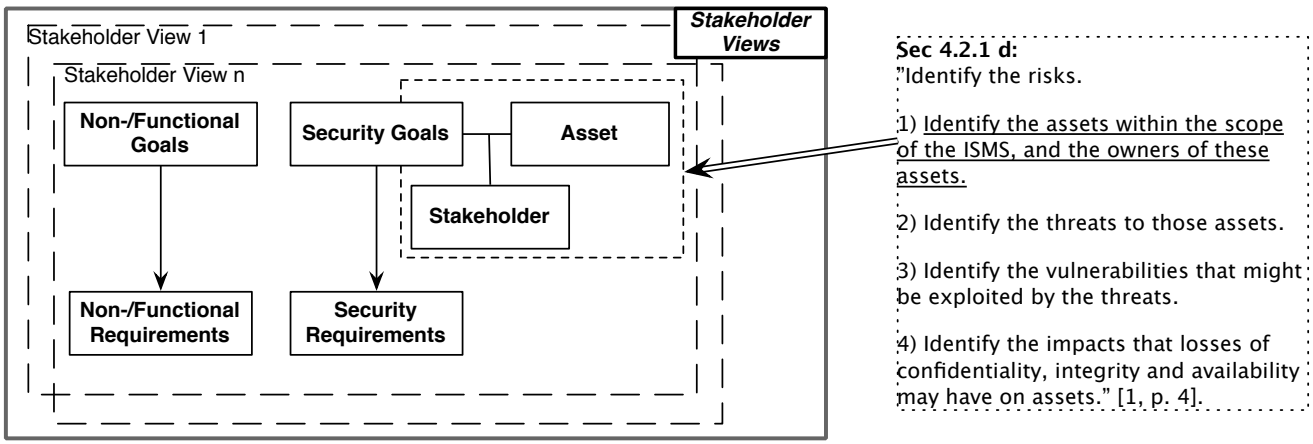

Figure 1: Matching the Conceptual Framework from Fabian et al. [6] and ISO 27001 Sect. 4.2.1 d (1/2)

ments engineering methods, e.g., identification of stakeholders, assets, vulnerabilities, and threats [5, p. 4].

The first part of the ISO 27001 Sect. 4.2.1 d demands an "identification of assets within the scope of the ISMS, and the owners of these assets. "[5, p. 4]. The CF property *Stakeholder Views* describes stakeholders and their assets. Fig. 1 shows this relation. For space reasons, we did not include figures for the previous relations. In addition, the relation of the scope and boundaries of the ISMS and the CF property *Stakeholder Views* is already elicited in Sect. IV-C.

Fig. 2 present the remaining relations between the ISO 27001 Sect. 4.2.1 d and the *Threat Analysis* property of CF. ISO 27001Sect. 4.2.1 d prescribes an identification of threats in relation to assets [5, p. 4]. Assets are not explicitly part of the *Threat Analysis* property of the CF. However, they are already considered in the *Stakeholder Views* property and linked to a stakeholder. The stakeholder is in turn a part of the *Threat Analysis* property. In addition, stakeholders require security properties, that can be violated by vulnerabilities. These are potentially exploited by threats. Thus, we have a relation to the *Threat Analysis* property. Moreover, ISO 27001 Sect. 4.2.1 d demands an identification of vulnerabilities to threats [5, p. 4]. As mentioned above, vulnerabilities are part of the *Threat Analysis* property.

Table IV: SRE methods supporting ISO 27001 Sect. 4.2.1 d

	Stakeholder Views	Threat Analysis	Risk Management
KAOS	x	x	
Secure Tropos	x		
SEPP			
CORAS		x	x

Furthermore, ISO 27001 Sect. 4.2.1 d provides an identification of impacts of losses [5, p. 4]. The loss to a stakeholder of a security property constitutes a risk in the *Threat Analysis* property of the CF. This is also an obvious connection to the risk management, which is a major property of ISO 27001 Sec. 4.2.1 d. In addition, ISO 27001 Sect. 4.2.1 d considers using security goals, the CIA tirade (confidentiality, integrity, availability), to describe the loss of a stakeholder that can be caused by a risk. This is not part of the graphical representation of the CF, however, the author‘s state that security goals in the CF have to be written down in terms of the CIA triad [6, p. 12]. Moreover, a security property contains among others security goals [6, p. 11,p. 14].

We presented the implementation of *Stakeholder Views* by the methods KAOS and Secure Tropos in Sect. IV-C. We now focus on *Risk Management* and the CORAS method that implements it. The CORAS method identifies assets, vulnerabilities and subsequent threats, followed by a risk analysis and treatment. Hence, the method is an almost perfect match for implementing ISO 27001 Sect. 4.2.1 d. The method does not consider *Stakeholder Views*. However, *Stakeholder Views* are included in the goal-oriented methods KAOS and Secure Tropos. These methods, on the other hand, do not explicitly consider *Risk Management*.

V. Practical Application of our Results

Developing an ISMS for a scenario, given a setting in the real world, is difficult, due to the sparse descriptions in the ISO 27001 standard. We support the establishment of an ISMS for a given scenario with two different use cases, derived from our results. The use cases, as discussed in Sect. I, are a top-down and a bottom-up procedure. The first use case is to apply SRE methods to systematically support an ISO 27001 establishment and implementation, hence a *top-down* approach. The second use case is to re-use SRE

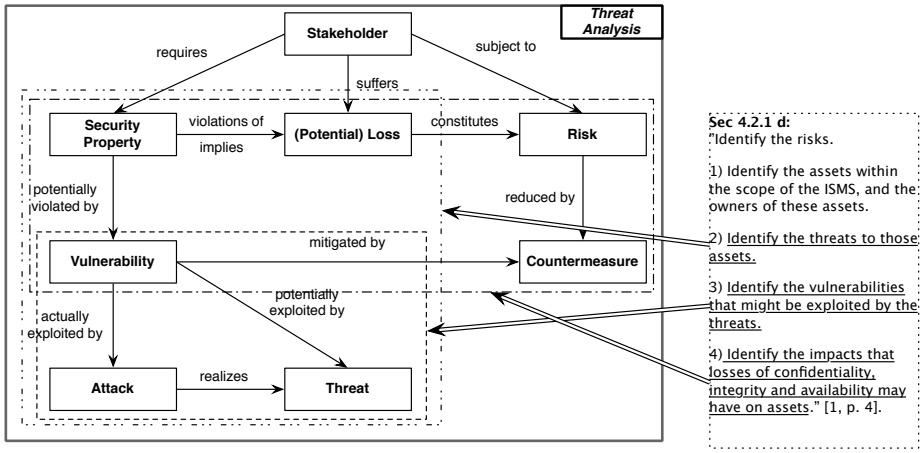

Figure 2: Matching the Conceptual Framework from Fabian et al. [6] and ISO 27001 Sect. 4.2.1 d (2/2)

documentation generated in former activities, which applied SRE methods, hence a *bottom-up* approach. Combinations of these use cases are possible.

The application of the result of our work within an ISO 27001 compliant ISMS establishment and implementation, is depicted in Fig. 3. The white area of the UML activity diagram contains the basic steps of an ISO 27001 process with the additional pre-phase from the ISO 27005, as described in Sect. II. The dark grey area depicts the bottom-up use case, and the light grey area the top-down use case.

The **top-down** use case supports most parts of the ISO 27001 process, using SRE methods. Therefore, we select the sections of the ISO 27001 we want to refine via SRE methods. Next, we select matching SRE methods by using Table III as we presented in Sections IV-C, and IV-D. As a next step, we use the selected SRE methods. We derive the parts of the resulting documentation that are relevant for establishing and implementing of an ISMS, according to ISO 27001. In addition, we can re-describe existing software related to the ISMS using SRE methods.

For the **bottom-up** use case, we have to check if there were any SRE methods used in former activities, e.g. when developing any kind of software related to the ISMS to be built. For existing SRE documents, we have to check if the applied SRE method is already considered within this work. If this is not the case, we have to establish this relation between the SRE method and the CF using the work of Fabian et al. [6]. After the relation is established, we are able to derive ISO 27001 supporting parts from the SRE documentation according to Table III. Furthermore, we can map the relevant ISO 27001 sections to the derived parts of the documentation.

VI. Conclusion

We have established a relation between the ISO 27001 standard and SRE methods. Thereby we build on the CF of Fabian et al. [6], which already established relations between the CF's terms and notions of several SRE methods. We contribute further relations from the ISO 27001 standard to the CF. The two sets of relations can be combined to identify suitable SRE methods for establishing an ISMS compliant with ISO 27001.

Our approach offers the following main benefits:

- Re-using SRE methods to support the development and documentation of security standards (here: ISO 27001)
- Systematic identification of relevant SRE methods for an ISO 27001 section
- Improving the outcome of ISO 27001 implementation by supporting establishment and documentation of an ISMS
- Re-using the structured techniques of SRE methods for analyzing and elicitating security requirements to support the refinement of sparsely described sections of the ISO 27001 standard

The work presented here will be extended to support further security standards . Moreover, we will look into extensions of SRE methods in order to be able to support the management and auditing demands of the ISO 27001 standard.

We also aim at an integration of SRE methods and other standard related methods. Such methods ease the work with a standard at hand and they have the potential to close gaps left open by an SRE method. This information is likely to be useful for the context description needed for the ISO 27001 standard documentation.

References

[1] ISO/IEC, "Information technology - Security techniques - Information security management systems - Overview and Vocabulary," International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27000, 2009.

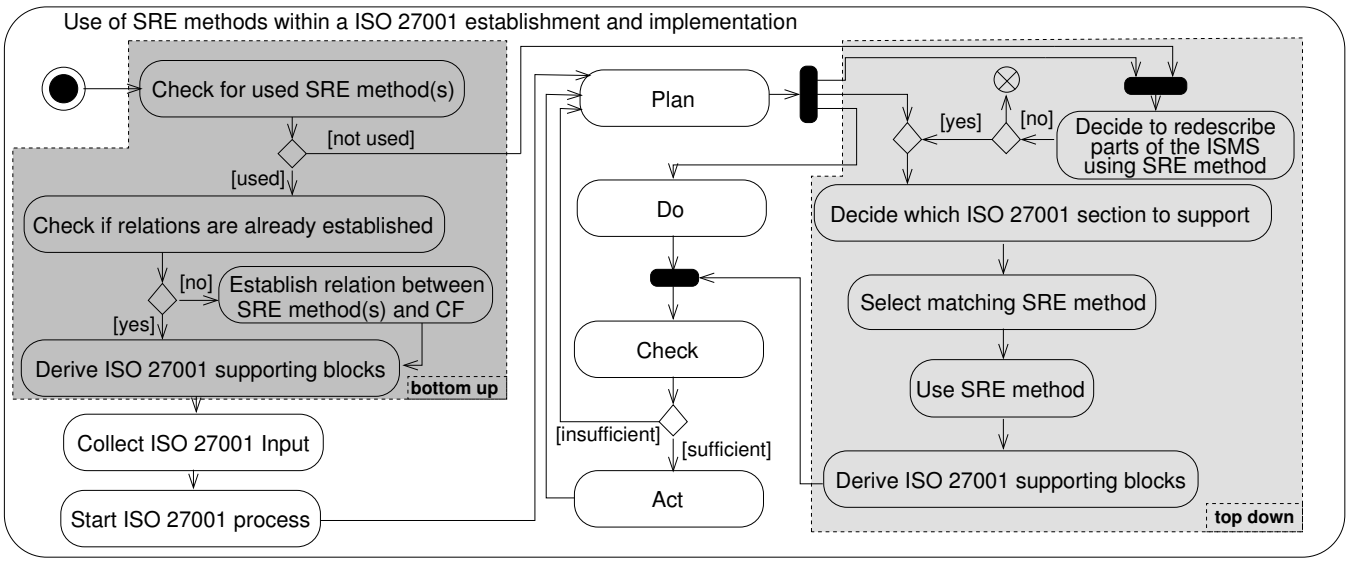

Figure 3: Practical application of this work within an ISO 27001 implementation

[2] H. Kersten, J. Reuter, and K.-W. Schröder, *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz*. Vieweg+Teubner, 2011.

[3] A. Calder, *Implementing Information Security based on ISO 27001/ISO 27002: A Management Guide*. Haren Van Publishing, 2009.

[4] ISO/IEC, "Information technology - security techniques - information security risk management," International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27005, 2008.

[5] ——, "Information technology - Security techniques - Information security management systems - Requirements," International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27001, 2005.

[6] B. Fabian, S. Gürses, M. Heisel, T. Santen, and H. Schmidt, "A comparison of security requirements engineering methods," *Requirements Engineering – Special Issue on Security Requirements Engineering*, vol. 15, no. 1, pp. 7–40, 2010.

[7] P. Karpati, G. Sindre, and A. L. Opdahl, "Characterising and analysing security requirements modelling initiatives," in *Proceedings of the International Conference on Availability, Reliability and Security (ARES)*. IEEE Computer Society, 2011, pp. 710–715.

[8] M. Jackson, *Problem Frames. Analyzing and structuring software development problems*. Addison-Wesley, 2001.

[9] ISO/IEC, "Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security," International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 13335-1, 2004.

[10] K. Beckers, S. Faßbender, M. Heisel, J.-C. Küster, and H. Schmidt, "Supporting the development and documentation of ISO 27001 information security management systems through security requirements engineering approaches," in *Proceedings of the International Symposium on Engineering Secure Software and Systems (ESSoS)*, ser. LNCS. Springer, 2012, pp. 14–21.

[11] A. van Lamsweerde, "Engineering requirements for system reliability and security," *Software System Reliability and Security, M. Broy, J. Grunbauer and C.A.R. Hoare (eds.), NATO Security through Science Series - D: Information and Communicarion Security*, vol. 9, pp. 196–238, 2007.

[12] P. Bertrand, R. Darimont, E. Delor, P. Massonet, and A. van Lamsweerde, "Grail/kaos: an environment for goal drivent requirements engineering," in *Proceedings 20th International Conference on Software Engineering (ICSE)*. IEEE ACM, 1998.

[13] A. Susi, A. Perini, J. Mylopoulos, and P. Giorgini, "The tropos metamodel and its use," *Informatica*, vol. 29, pp. 401–408, 2005.

[14] H. Mouratidis and P. Giorgini, "Secure tropos: a security-oriented extension of the tropos methodology." *International Journal of Software Engineering and Knowledge Engineering*, vol. 17, no. 2, pp. 285–309, 2007.

[15] H. Schmidt, D. Hatebur, and M. Heisel, "A pattern- and component-based method to develop secure software," in *Software Engineering for Secure Systems: Academic and Industrial Perspectives*, H. Mouratidis, Ed. IGI Global, 2011, ch. 3, pp. 32–74.

[16] M. S. Lund, B. Solhaug, and K. Stølen, *Model-Driven Risk Analysis: The CORAS Approach*, 1st ed. Springer Publishing Company, Incorporated, 2010.