Supporting the Development and Documentation of ISO 27001 Information Security Management Systems through Security Requirements Engineering Approaches*

Kristian Beckers[1], Stephan Faßbender[1], Maritta Heisel[1], Jan-Christoph Küster[2], and Holger Schmidt[1]

[1] paluno - The Ruhr Institute for Software Technology University of Duisburg-Essen
firstname.lastname@paluno.uni-due.de
[2] Fraunhofer Institut for Software and Systems Engineering ISST
Jan-Christoph.Kuester@isst.fraunhofer.de

Abstract. Assembling an information security management system according to the ISO 27001 standard is difficult, because the standard provides only sparse support for system development and documentation.

We analyse the ISO 27001 standard to determine what techniques and documentation are necessary and instrumental to develop and document systems according to this standard. Based on these insights, we inspect a number of current security requirements engineering approaches to evaluate whether and to what extent these approaches support ISO 27001 system development and documentation. We re-use a conceptual framework originally developed for comparing security requirements engineering methods to relate important terms, techniques, and documentation artifacts of the security requirements engineering methods to the ISO 27001.

Keywords: Security standards, requirements engineering, ISO27000, ISO27001, compliance, security.

1 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,

* This research was partially supported by the EU project Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS, ICT-2009.1.4 Trustworthy ICT, Grant No. 256980).

G. Barthe, B. Livshits, and R. Scandariato (Eds.): ESSoS 2012, LNCS 7159, pp. 14–21, 2012.

or usage scenarios, of the ISMS in detail [1]. For example, the ISO 27005 [2] 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"[3, 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. 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 addresses the research question, if and to what extent SRE approaches can support the development of an ISO 27001 compliant ISMS. Moreover, it addresses the question in what way SRE methods provide 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 2 presents background on the ISO 27001 standard, and Sect. 3 presents the CF of Fabian et al. [4]. We set up a relation between the ISO 27001 standard and the conceptual framework (CF) in Sect. 4. In addition, we obtain a relation of security requirements methods to the ISO 27001. Section 5 provides insights into the results of the relations and Sect. 6 presents related work. Section 7 concludes and gives directions for future research.

2 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* [3]. 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 [2] refines this process for risk management and extends it with a pre-phase for information gathering.

3 A Conceptual Framework for Security Requirements Engineering

Notions and terminology differ in different SRE methods In order to be able to compare different SRE methods, Fabian et al. [4] 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. [5, p. 714] 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. [4]. 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 [6], 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.

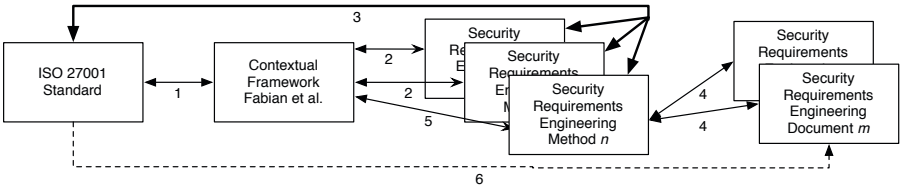

Fig. 1. Relating security requirements engineering methods with the ISO 27001

4 Relating the ISO 27001 Standard and Security Requirements Engineering Methods

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. We depict the analysis in Fig. 1. First, we create a relation between the ISO 27001 standard and the CF of Fabian et al. [4]. 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* (step 4). 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 yet exist, we have to create it (step 5). 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 (step 6).

Note that the ISO 27001 sparsely describes the structure and content of an ISO 27001 compliant documentation. Thus, a relation between a specific artifact generated by a SRE method and a certain part of the documentation required by the ISO 27001 cannot firmly be established. It is up to the auditors to decide if an artifact fully fulfills an ISO 27001 documentation need.

Table 1 relates relevant terms for security from the CF by Fabian et al. [4] to the ISO 27001 standard. The matching benefits from the fact that both documents rely on ISO 13335 [7] definitions for several terms.

ISO 27001 Section 4 describes the ISMS. Hence, we focus on this section in particular. Table 2 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

Table 1. Correspondence between ISO 27001 terms and terms of the CF [4]

CF Fabian et al.	**ISO 27001**
System	The *organisation* is the "scope"of the standard [3, p. 1].
Machine	The *Information Security Management System (ISMS)* is the machine to be built [3, p. v].
Environment	The *scope and boundaries* of the "organization"[3, p. 4, Sec 4.2.1 a] relevant for the ISMS.
Security Goal	The standard uses *security objectives* [3, 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 [3, p. v,vi].
Specification	The ISMS's policy, controls, processes and procedures [3, p. vi] are the specification of the machine.
Stakeholder	The *Interested Parties* [3, 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* [3, p. 4].
Availability	The definition in ISO/IEC 13335 [7] is also used [3, p. 2].
Confidentiality	The definition in ISO/IEC 13335 [7] is also used [3, p. 2].
Integrity	The definition in ISO/IEC 13335 [7] is also used [3, p. 2].
Asset	The definition in ISO/IEC 13335 [7] is also used [3, p. 2].
Threat	The definitions match. Threats are defined towards assets and threats exploit vulnerabilities [3, p. 4].
Vulnerability	The definitions match [3, p. 4].
Risk	The CF defines risk as "the potential loss of a stakeholder"[4, 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 [3, p. 4]. Hence, we can conclude that the meaning is similar.

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 [2]. A "+"in Tab. 2 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.

5 Insights

We presented a relation between SRE methods and the ISO 27001 standard. The relations were obtained via the CF of Fabian et al. [4]. This CF presents four distinct building blocks of SRE methods. Table 2 relates the ISO 27001 standard to these building blocks. The *Stakeholder Views* building block has multiple relations to ISO 27001 sections. The reason is that the counterparts in the standard focus on the view of the organization including its stakeholders. The *Stakeholder Views* are part of numerous goal-oriented approaches, e.g., Secure Tropos [8] and KAOS [9]. This is no surprise, because these methods often derive their goals from the views of stakeholders.

Also the *Threat Analysis* building block has multiple counterparts in the ISO 27001. The reason for these is the strong emphasis of the standard on risk, which is part of that building block. Thus, risk management-oriented approaches, such as CORAS [10], play a crucial role in an ISO 27001 assembly. The problem-oriented approaches, e.g. SEPP [11], are useful for the structured collection of knowledge about the environment that must be considered.

Table 3 presents the mandatory documents for an ISO 27001 documentation according to [3, p.13]. In addition, Tab. 3 shows the kinds of SRE methods that support the assembly of these documents. The table is based upon our analysis in Sect. 4.

Table 2. Relating ISO 27001 Section 4 to CF building block

Section	Description	SV	SR	SDK	TA	RM
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), **RM**(Risk Management)

Table 3. Support of SRE Methods for ISO 27001 documentation

Documentation Requirements ISO 27001	Support from SRE Methods
ISMS policies and objectives	Goal-/Problem-/Risk-oriented methods
Scope and boundaries of the ISMS	Goal-/Problem-/Risk-oriented methods
Procedures and controls	Risk-oriented methods
The risk assessment methodology	Risk-oriented methods
Risk assessment report	Risk-oriented methods
Risk treatment plan	Risk-oriented methods
Information security procedures	Goal-/Problem-oriented methods
Control and protection of records	No support from SRE methods
Statement of Applicability	Goal-/Problem-/Risk-oriented methods

6 Related Work

Mondetino et al. investigate possible automation of controls that are listed in the ISO 27001 and ISO 27002 [12]. Beckers et al. [13] propose a common pattern for the cloud computing domain to support context establishment and asset identification of the ISO 27000 series. Both works can complement our own.

7 Conclusion

We have established a relation between the ISO 27001 standard and SRE methods. Thereby we build on the CF of Fabian et al. [4], 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) compliant systems
- 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

In the future 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.

Acknowledgements. We thank Denis Hatebur for his extensive and valuable feedback on our work.

References

1. ISO/IEC: Information technology - Security techniques - Information security management systems - Overview and Vocabulary. ISO/IEC 27000, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2009)
2. ISO/IEC: Information technology - security techniques - information security risk management. ISO/IEC 27005, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2008)
3. ISO/IEC: Information technology - Security techniques - Information security management systems - Requirements. ISO/IEC 27001, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2005)
4. Fabian, B., Gürses, S., Heisel, M., Santen, T., Schmidt, H.: A comparison of security requirements engineering methods. Requirements Engineering – Special Issue on Security Requirements Engineering 15(1), 7–40 (2010)
5. Karpati, P., Sindre, G., Opdahl, A.L.: Characterising and analysing security requirements modelling initiatives. In: Proceedings of the International Conference on Availability, Reliability and Security (ARES), pp. 710–715. IEEE Computer Society (2011)
6. Jackson, M.: Problem Frames. Analyzing and structuring software development problems. Addison-Wesley (2001)
7. ISO/IEC: Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security. ISO/IEC 13335-1, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2004)
8. Mouratidis, H., Giorgini, P.: Secure tropos: a security-oriented extension of the tropos methodology. International Journal of Software Engineering and Knowledge Engineering 17(2), 285–309 (2007)
9. van Lamsweerde, A.: Engineering requirements for system reliability and security. In: Broy, M., Grunbauer, J., Hoare, C.A.R. (eds.) Software System Reliability and Security. NATO Security through Science Series - D: Information and Communicarion Security, vol. 9, pp. 196–238 (2007)
10. Lund, M.S., Solhaug, B., Stølen, K.: Model-Driven Risk Analysis: The CORAS Approach, 1st edn. Springer, Heidelberg (2010)
11. Schmidt, H., Hatebur, D., Heisel, M.: A pattern- and component-based method to develop secure software. In: Mouratidis, H. (ed.) Software Engineering for Secure Systems: Academic and Industrial Perspectives, pp. 32–74. IGI Global (2011)
12. Montesino, R., Fenz, S.: Information security automation: how far can we go? In: Proceedings of the International Conference on Availability, Reliability and Security (ARES), pp. 280–285. IEEE Computer Society (2011)
13. Beckers, K., Küster, J.C., Faßbender, S., Schmidt, H.: Pattern-based support for context establishment and asset identification of the ISO 27000 in the field of cloud computing. In: Proceedings of the International Conference on Availability, Reliability and Security (ARES), pp. 327–333. IEEE Computer Society (2011)