Supporting the Context Establishment according to ISO 27005 using Patterns

Kristian Beckers, Stephan Faßbender
paluno - The Ruhr Institute for Software Technology -
University of Duisburg-Essen, Germany

Kristian.Beckers,Stephan.Faßbender@paluno.uni-due.de

Abstract: The documentation of an information and communication system according to the requirements of the ISO 27005 standard is difficult, because the standard only provides sparse descriptions.

We propose the use of specific patterns for the ISO 27005 standard, which can be instantiated for any given information and communication system. Each of our pattern will cover a section of the standard. In this paper we present one pattern for Section 7 of the standard, the context establishment. This is one of the initial steps of the standards and it is the input for following steps, e.g., the asset identification.

1 Introduction and Background

Establishing trust of customers is essential for a company. The security level of a company is a decisive factor in establishing this trust. The ISO 27000 series of security standards supports to achieve this goal.

In this paper we provide patterns for the context establishment of the security information risk management process according to the ISO 27005 [ISO08] standard. The importance of this step is obvious, because later steps depend upon it. Beckers et al. [BKFS11] proposed a common pattern for the cloud computing domain to support context establishment and asset identification of the ISO 27000 series. We built upon this work an present a more general approach that is not limited to cloud computing systems, but support any kind of ICT system. Moreover, the work in [BKFS11] only extends to parts of the context establishment, the patterns presented in this work cover the entire context establishment.

The ISO 27001 defines the requirements for for establishing and maintaining an ISMS [ISO05]. In particular the standard describes the process of creating a model of the entire business risks of a given organization and specific requirements for the implementation of security controls. The resulting ISMS provides a customized security level for an organization.

The ISO 27001 standard is structured according to the “Plan-Do-Check-Act” (PDCA) model, the so-called *ISO 27001 process* [ISO05]. 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 [ISO08] refines this process for risk management and extends it with a pre-phase for information gathering.

The process starts with a gathering of information about the organization. The next activity is the *context establishment*. This initial step is important for all following steps and is responsible, whether the risk management can be implemented in a sufficient extent and on a sufficient level of detail. The next step is the *risk identification*, that determine potential loss. Then *risk estimation* tries to rate the consequences of loss on a qualitative or quantitative scale as well as the likelihood of occurrence. The *risk evaluation* step compares the level of risks against the risk acceptance criteria, defined during the context establishment. Then, the *risk treatment* step sets up controls. In the *risk acceptance* step, residual risks have to be accepted by managers of the organisation.

2 Supporting Context Establishment using Patterns

In our previous work [BKFS11] we presented a cloud system analysis pattern that provides a conceptual view on cloud computing. The pattern supports to systematically instantiate stakeholders, cloud technology, and relations between these. The instantiated pattern allows a structured analysis of cloud stakeholders and the cloud system. The documentation can be used for parts of the early phases of the ISO 27005 standard. We propose in this work a generic version of the cloud system analysis pattern, which can be instantiated for any given ICT system, depict in Fig. 1.

An ICT system is a software system that processes data for stakeholders. The software system consists of resources that have a location and the system consists of hardware and software. The system is embedded into a direct system environment, which contains stakeholders that have a direct relation to the system. The direct system environment is further embedded into the indirect system environment, which contains stakeholders that have no direct relation to the system.

The *System Owner* owns the ICT system, the *Administrator* maintains the resources of the software system. The *Developers* develops software for the ICT system. The system has an *Internal Users* that works for the System Owner and exchanges data with the ICT system. In addition, *External Users* work for a *Customer* of the System Owner.

The stakeholder of the indirect environment are the legislator, a set of all relevant laws from a specific country. The template can be instantiated with multiple legislator of all the countries relevant for the ICT system. The domain represents a set of all relevant regulations for, e.g., the finance domain.

We accompany the system analysis pattern by templates to systematically gather domain knowledge about the direct and indirect system environments based upon the stakeholders' relations to the system and other stakeholders. This is also similar to the approach in

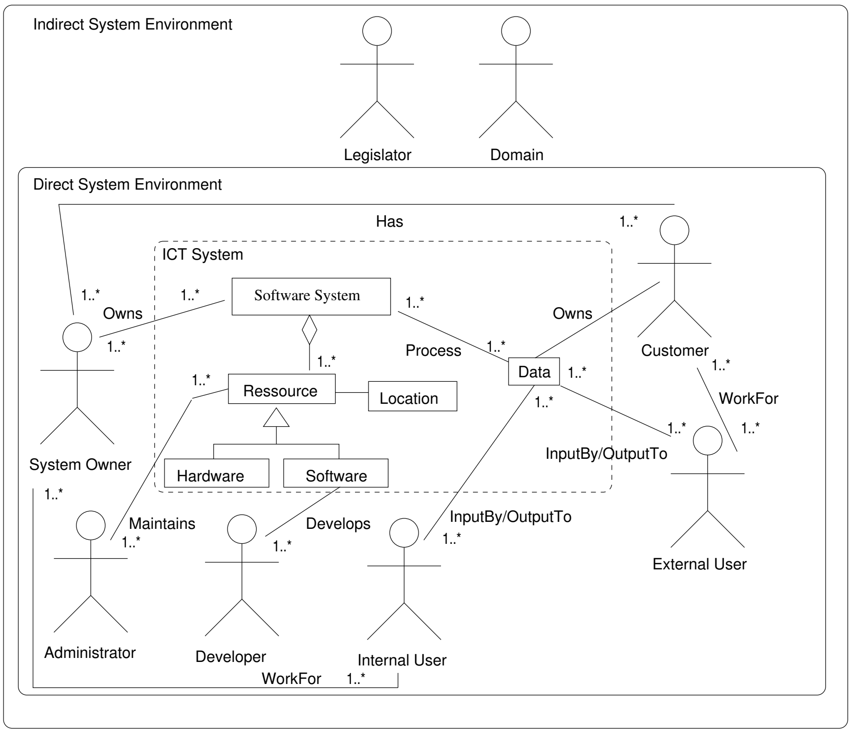

Figure 1: System Analysis Pattern

[BKFS11].

We present a template for the administrator as an example for the templates for the indirect stakeholders:

Name Administrator

Description The administrator repairs the system and he/she executes maintenance efforts.

Relations to the ICT system The administrator has access to the entire data in the system.

Motivation The administrator earns money by maintaining the resources of the ICT system.

Relations to other direct stakeholders The administrator has a contract with the System Owner to maintain the system. There might also be further contracts, e.g., preventing the administrator from accessing the Customers data.

Assets The administrator has no direct assets in the ICT system. However, if the ICT system does not exist, he/she would not earn money. Hence, the system itself could be considered the asset of the administrator.

When the gathering of information about the organization is done, the ISO 27005 demands a context establishment as a next step. We present an *ISO 27005 Context Establishment Pattern*, depict in Fig. 2. This contains several vital parts of the ISO 27005 context establishment and considers the basic process of this part of the standard. This pattern can be

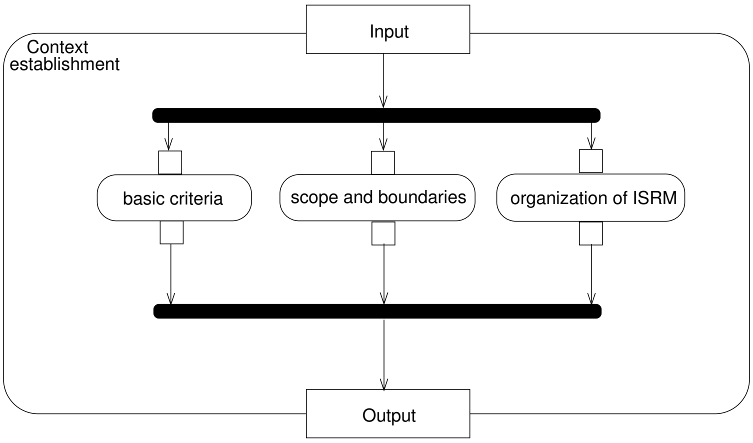

Figure 2: ISO 27005 Context Establishment Pattern

instantiated systematically for a given organization. The resulting instance of the pattern can be used as documentation for the standard implementation. The pattern contains three elements of the standard, which have to be instantiated. These parts are the *basic criteria*, the *scope and boundaries* and the *organization of information security risk management (ISRM)*.

The basic criteria is instantiated with a set of resources, which have to be elicited before the instantiation. Resources according to the ISO 27005 standards are all relevant elements of an organization to the ISRM. We propose to use our system analysis pattern as a source for these resources. The basic critera requires further that information assets have to be derived from the set of resources. Afterwards the resulting set of information assets has to be refined to classes of similar information assets. For each of these classes an assesment of security breaches has to be conducted. This shall be done for at least the following kinds of security issues: CIA breaches, financial and business loss, compliance breaches. Afterward criteria have to developed for each class of information assets based on the assessed breaches and losses. Those criteria should include risk evaluation criteria, impact criteria and risk acceptance criteria.

The scope and boundaries has to be instantiated with collected information artifacts about organization. These artifacts have to be collected from: business objectives, strategies, information security policies, business processes, organizational functions and structure, legal and contractual requirements, stakeholders and their expectations, socio-cultural environment, and interfaces between environment and organization. For each collected information artifact, it has to be decided whether it shall be included in the scope and boundaries (or not).

An information security risk management process has to be defined and documented, as part of the description of the organization of the ISRM. Such a process should contain the stakeholders of the system, the roles they enact, the activities they execute, the relations between stakeholders, roles and the organization, and the records to be kept. Our system analysis pattern already defines most of the needed information in a coarse grained way.

We accompany the ISO 27005 Context Establishment Pattern also with templates to systematically gather the requested knowledge for the basic criteria, scope and boundaries, and organization of ISRM. We provide the template for the organization of the ISRM process as an example:

Stakeholder As defined in the system analysis pattern

Roles

- **Rolename** A short name of the role
- **Description** A summarizing description of the role
- **Stakeholder** A list of stakeholders which can enact the role
- **Precondition** Conditions to be fulfilled to enact this role.
- **Responsibilities** A description for which assets and resource the role is responsible
- **Rights** A description of rights the role has to have to fulfill the responsibilities.
- **Excluded roles** A list of role,s which are not allowed to be bound to a stakeholder, who enacts the role at hand, at the same time.

Resources And Assets

- **Name** Identifier for the resource or asset
- **Description** A summarizing description of the resource or asset
- **Stakeholder** A list of stakeholders, which have a relation to the resource or assets. The relation has also to be described

Records

- **Identifier** Identifier for the record
- **Description** A summarizing description of record
- **Template** A template to generate a record
- **Instantiation Description** A description to instantiate te template

Activities

- **Activity** A short name of the activity
- **Description** A summarizing description of the activity
- **Precondition** Activities and constrains to be fulfilled before this activity can be executed.
- **Affected Stakeholders** A list of stakeholders which are affected by the activity
- **Roles** The roles which are allowed to execute this activity
- **Resources and Assets** A list of resources and assets which are necessary for the activity
- **Records** List of records to be generated when this activity is executed
- **Postcondition** Activities and constrains to be fulfilled after this activity has been executed

3 Related Work

Cheremushkin et al. [LCAS11] present a UML-based meta-model for several terms of the ISO 27000, e.g., assets. These meta-models can be instantiated and, thus, support the refinement process. However, the authors do not present a holistic approach to information security. The work mostly constructs models around specific terms in isolation. Mondetino et al. investigate possible automation of controls that are listed in the ISO 27001 and ISO 27002 [MF11]. Their work can complement our own.

4 Conclusions and Future Work

We presented a pattern for the context establishment section for the ISO 27005 standard. Our work shows that the ISO 27005 can benefit from a system of patterns that can be instantiated for any given ICT system. Our approach comprises the following main benefits: A generic context establishment based on patternsa and systematic pattern-based documentation of ICT systems. This benefits ease the burden of establishing the context for a ISO 27005 certification. In the future we will extend our work for the entire ISO 27005 standard. In addition, we intend to develop a general method to support the establishment of security standards, and apply it for instance as validation to the BSI Standard 100-2.

References

[BKFS11] Kristian Beckers, Jan-Christoph Küster, Stephan Faßbender, and Holger Schmidt. 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)*, pages 327–333. IEEE Computer Society, 2011.

[ISO05] 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.

[ISO08] ISO/IEC. Information technology - Security techniques - Information security risk management. ISO/IEC 27005, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), 2008.

[LCAS11] Alexander Lyubimov, Dmitry Cheremushkin, Natalia Andreeva, and Sergey Shustikov. Information security integral engineering technique and its application in ISMS design. In *Proceedings of the International Conference on Availability, Reliability and Security (ARES)*, pages 585–590. IEEE Computer Society, 2011.

[MF11] Raydel Montesino and Stefan Fenz. Information security automation: how far can we go? In *Proceedings of the International Conference on Availability, Reliability and Security (ARES)*, pages 280–285. IEEE Computer Society, 2011.