# Goal-Based Establishment of an Information Security Management System Compliant to ISO 27001*

Kristian Beckers

Paluno, - The Ruhr Institute for Software Technology -, University of Duisburg-Essen, Germany
{firstname.lastname}@paluno.uni-due.de

**Abstract.** It is increasingly difficult for customers to understand complex systems like clouds and to trust them with regard to security. As a result, numerous companies achieved a security certification according to the ISO 27001 standard. However, assembling an Information Security Management System (ISMS) according to the ISO 27001 standard is difficult, because the standard provides only sparse support for system development and documentation.

Security requirements engineering methods have been used to elicit and analyse security requirements for building software. In this paper, we propose a goal-based security requirements engineering method for creating an ISMS compliant to ISO 27001. We illustrate our method via a smart grid example.

**Keywords:** security standards, requirements engineering, SI*.

## 1 Introduction

The increasing complexity of software systems and the surrounding environment is challenging to analyse with regard to security. Security standards, e.g. the ISO 27001 standards, offer a way to attain this goal. The ISO 27001 standard defines how to establish an information security management system (ISMS). This is a concern for the security needs of an organisation. Several relevant companies have taken this approach like Amazon[1]. However, the sparse descriptions in it makes the establishment of an ISO 27001 compliant ISMS difficult. For example, the standard contains a description of the scope and boundaries of the ISMS. The standard states only to consider "characteristics of the business, the organisation, its location, assets and technology" [1, p. 4].

Re-using well established methods security requirements engineering (SRE) methods, e.g., SI* [2] for establishing an ISMS according to the ISO 27001 is a possible solution. We provided a mapping from the ISO 27001 standards demands to the capabilities of SRE methods in a previous work [3].

This work is inspired by this mapping and shows how to use SI* for establishing an ISO 27001 ISMS. Our approach provides a structured refinement of the IT system's and stakeholders' information to assess the threats for a particular system. Our method

* 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). We thank Jorge Cuéller for his valuable feedback on our work.

[1] http://aws.amazon.com/security/

V. Geffert et al. (Eds.): SOFSEM 2014, LNCS 8327, pp. 102–113, 2014.

uses this information for risk assessment and security control selection according to the ISO 27001 standard. We also provide the required documentation of an ISMS for certification. We illustrate our approach by the example of a smart grid providing scalable energy infrastructure to consumers. We consider in particular the security of the smart metering gateway, the interface between the energy grid and the customer.

## 2 ISO 27001

The ISO 27001 standard is structured according to the "Plan-Do-Check-Act" (PDCA) model, the so-called *ISO 27001 process* [1]. 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*.

## 3 SI*

We use the SI* modeling language [2] for creating a refined ISMS scope definition, because SI* provides the means to model social dependencies between actors including security and trust relations. In SI* roles are abstractions of sets of actors, which are active entities that have goals. A goal is a state of affairs that the actor desires and that the system-to-be should possibly help to fulfill. Softgoals are similar, but have no clear criteria for stating if they are fulfilled or not. A resource is a physical or informational entity. Goals and resources can be refined using *AND decomposition*s, these have the word AND under a half circle. A *means-end* is an arrow that points towards a goal that provides the means to achieve a goal or the resources needed or produced by a goal.

Own relations denote that an actor owns a resource, or can decide if a goal is achieved. This relation is labeled with an **O**. Provide relations denote that an actor has the ability to achieve a goal or furnish a resource. This relation is labeled with a **P**. The own and provide relations are part of the so-called *Eco Model*.

SI* supports various trust relations, which are modelled as edges labeled with an abbreviation of the kind of trust relation it represents. Execution dependency **De** and permission delegation **Dp** allow the transfer of objectives and entitlements from an actor to another. Execution dependency **De** means that one actor appoints another actor to achieve a goal or furnish a resource. Permission delegation **Dp** indicates that an actor authorises another actor to achieve a goal or deliver a resource. Trust is a relation representing the expectations that an actor (the trustor) has in regards to the behavior of another actor (the trustee). A goal or a resource is part of a trust relation (the trustum). Trust of execution **Te** models the trustor's expectations regarding the ability and dependability of the trustee in fulfilling a goal or delivering a resource. Trusting in execution **Tp** means that the trustor is certain that the trustee accomplishes the trustum. Trust of permission models the trustor's expectations that the trustee does not abuse a goal or a resource. Trusting in permission means that the trustor is certain that the trustee does not misuse the (possible) received permission for accomplishing an aim different from the one for which the permission has been granted. Distrust execution **Se** models the explicit doubts about the behaviour of the trustor from the trustee about the abuse of a goal or a resource.

## 4 A Method for Goal-Based ISMS Establishment

We propose a method for creating an ISMS compliant to the ISO 27001 standard, which consists of the following steps:

**Step 1: Get Management Commitment -** The precondition for building an ISMS is that the management commits to it. Thus, we dedicated the first step of our method to elicit the management commitment of the project and the provision of adequate resources to do so. We create SI* diagrams that state the concerned roles and actors of an ISMS. The management commitment for an ISMS shall be granted for these roles and actors. The management commitment has to be gathered repeatedly when the ISMS is further described. However, starting from the initial definition of concerned stakeholders a management commitment should be given in written form. Without this commitment, insufficient resources will result in an insufficient ISMS.

**Step 2: ISMS Scope Definition -** We define the scope of the ISMS using the SI* diagrams created in the previous step. Although, we could have used other goal modeling notations, SI* provides the means to model trust into a goal model, which is essential for our asset identification and threat analysis. In addition, SI* is scalable, since it is possible to have multiple diagrams/views of the same model.

**Step 3: Identify Assets -** The entire ISMS scope description is the input for the asset identification. We identify all items of value of stakeholders by analyzing various relations in the SI* model. These range from resource, goal, stakeholder relations to the trust relations in the SI* model. These also help to clearly define the need for protection of the identified assets. In addition, a high level risk assessment of the assets is conducted. This step results in a list of assets, the stakeholders that own them, and initial risk levels for assets as an output.

**Step 4: Analyze Threats -** We conduct a threat analysis via modeling attackers to these threats in the SI* model. Attackers have to be of a specific type, which contains assumptions about the capabilities and motivations of the attacker. These attackers present threats to assets. The threats lead to the elicitation of security requirements. We use misuse cases [4] to map the threats to security requirements.

**Step 5: Conduct Risk Assessment and Control Selection -** The reasoning about controls starts with the risk assessment for each asset. For each asset the decision has to be made if the risk to that asset demands the inclusion of one or more controls of the ISO 270001 standard or if the risk levels are sufficient. For each asset we propose to compile a list that states why a list of each of the controls in the normative ANNEX A of the ISO 27001 should or should not be applied to the asset.

**Step 6: Design ISMS Specification -** The final step of our method concerns the ISO 27001 specification, an implementable description of the ISMS. We consider the ISO 27001 documentation demands and use the information elicited and documented in the previous steps of our method. This information is mapped to the required document types for certification.

## 5 Application of Our Method to a Smart Grid Scenario

We illustrate the benefits of our framework on a case study of a Smart Grid system. The case study was provided by the industrial partners of the EU project NESSoS[2]. A smart grid is a commodity network that intelligently manages the behavior and actions of its participants. The commodity consists of electricity, gas, water, or heat that is distributed via a grid (or network). The benefit of this network is envisioned to be a more economic, sustainable, and secure supply of commodities. Smart metering systems meter the consumption or production of energy and forward the data to external entities. This data can be used for billing and steering the energy production.

**Step 1: Get Management Commitment -** The ISO 27001 standard demands documentation of management commitment for the establishment of an ISMS. The demands are described in Sect. 5 of the standard. *Sect. 5.1 Management Commitment* concerns proof that the management shall provide for establishing an ISMS including objectives, plans, responsibilities and accepting risks. *Section 5.2 Resource Management* concerns the provision of resources for establishing the ISMS and the training of the members of the organization for security awareness and competence.

The management commitment for implementing an ISMS according to the ISO 27001 standard is of utmost importance, because without the commitment of sufficient staff and resources the ISMS implementation is doomed to fail. In addition, the publicly available sources of examples of ISMS implementations, e.g., the ISMS toolkit, define this also as the first step when implementing an ISMS[3].

The management commitment should be based upon a high level description of the part of an organization for which the management commits resources to build an ISMS. We propose to use SI* diagrams for this purpose, because these define stakeholders and operations for which an ISMS shall be established. A refined description using static and behavioral description is done during the ISMS scope refinement (see below). We propose to mark the ISMS scope in the diagram. and use a scenario-based elicitation of stakeholders. The management commitment for establishing an ISMS for the scope has to be presented in writing and in relation to a specific person, who is responsible for providing the required resources. The management commitment should relate to the use case diagram, e.g., let the management commitment state that the service provider can provide services in a secure environment.

**Step 2: ISMS Scope Definition -** After acquiring the management commitment, we have to provide a more detailed scope definition. Section 4 of the ISO 27001 standard describes the ISMS and in particular in Sect. 4.2 - Establishing and managing the ISMS - states the scope definition. Section 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 "[1, p.4]. In Sect. 4.2.1 d, which concerns risk identification, the scope definition is used to identify assets. Section 4.2.3 demands a management review of the ISMS that also includes to check for possible changes in the scope of the ISMS. Section 4.3 lists the documentation demands of the standard and Sect. 4.3.1 d requires a

[2] http://www.nessos-project.eu/

[3] http://www.iso27001security.com/html/iso27k_toolkit.html

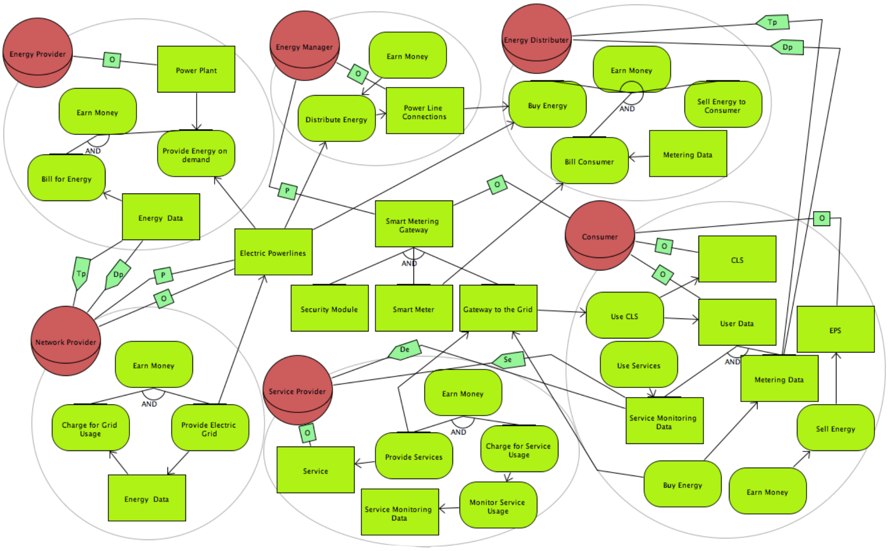

**Fig. 1.** Smart Grid SI* Diagram with Resources

documentation of the scope of the ISMS. The ISMS scope definition of the ISO 27001 standard is a vital step for its successful implementation, because all subsequent steps use it as an input.

We excluded the *Energy Market* from the scope of the ISMS and show the goals of the roles the ISMS is concerned with and their subgoals. These goals are shown in Fig. 1. Figure 1 presents a refined SI* diagram of our smart grid scenario. The *Energy Provider* owns *Power Plant*s and has the goal to *Earn Money*. The goal is decomposed into the subgoals to *Provide Energy on demand* and to *Bill for Energy* sales. In order to be able to bill for energy consumption, the *Energy Provider* has to acquire *Energy Data* that states the actual consumption of energy in the grid. Energy that is not consumed by a *Consumer* is an economic loss. Possible causes are loss of energy during transfer or just energy that fades in the grid, because of lack of energy storing capabilities. The *Energy Provider* has a delegation permission relation with the *Network Provider* for collecting the *Energy Data*. The *Energy Provider* trusts the *Network Provider*, because of long lasting partnership. Hence, both parties have a trust permission relation regarding the *Energy Data*.

The *Network Provider* also aims to *Earn Money* and this goal is decomposed into the goals *Charge for Grid Usage* and *Provide Electric Grid*. The *Provide Electric Grid* requires *Electric Powerlines*, which are owned and provided by the *Network Provider*. The *Energy Data* are an outcome of the realization of the goal *Provide Electric Grid*. The *Energy Data* are a means to achieve the goal *Charge for Grid Usage*.

The *Service Provider* also wants to *Earn Money* and does this via the subgoals *Provide Services* and *Charge for Service Usage*. The *Provide Services* goal leads to

*Services*, which are owned by the *Service Provider*. The *Charge for Service Usage* requires the subgoal *Monitor Service Usage*, which results in *Service Monitoring Data*. This data is collected from the *Consumer*. This is the reason why the *Service Provider* has an execution dependency relation with the *Consumer*. In addition, the *Consumer* is not familiar with the business practices of the *Service Provider*, which results in a distrust execution relation between these stakeholders.

The *Consumer* wants to *Buy Energy* and in addition *Use Services* and *Use CLS*, which are Controllable Local Systems (CLS). These are electronic components that use the *Smart Metering Gateway*. An example for a CLS is a controllable air conditioning. *CLS* devices are owned by the *Consumer*. The *Consumer* owns *User Data*. This data results from fulfilling the goal *Use CLS*. The *Use Service*s goal produces *Service Monitoring Data* that the *Energy Distributer* generates for billing purposes. The *Buy Energy* goal also results in *Metering Data* about energy consumption. The *Metering Data* is shared with the *Energy Distributer* using a delegation permission. The *Consumer* trusts the *Energy Distributer* to use this data only for billing purposes. The *Consumer* has also the goal to *Earn Money* via the subgoal *Sell Energy*. The *Consumer* uses an *EPS* for this purpose, which is an Energy Producing System. The *Customer* owns the *EPS*, which can be for example solar panels.

The *Energy Distributer* aims to *Earn Money* by the goal *Sell Energy to Consumer*s. The *Energy Distributer* wants to *Buy Energy*, which can be sold to *Consumer*s. The *Energy Manager* provides the energy from the grid, so that the *Energy Distributer*'s customers can receive it. The goal *Bill Consumer* requires *Metering Data* that state the amount of energy used by *Consumer*s. The *Energy Manager* owns *Power Line Connections* that are connected with the energy grid. These allow the *Energy Manager* to *Distribute Energy* throughout the grid.

The SI* model is an adequate description of an ISMS scope, because the SI* models describe the "characteristics of the business and the the organization" by analyzing and documenting goals, agents/roles including their relations. The standard also demands a documentation of the "technology" involved. These are included in the models via resources and its relations with goals and agents/roles.

The standard further demands the definition of "location". We propose to attach templates to the Si* model. The location template, shown in Tab. 1, lists the location of all Si* resources and agents/roles. Goals are not listed here, because these do not have physical locations. Moreover, the standard demands "details of and justification for any exclusions from the scope". We propose to use a scope exclusion template for that purpose that lists all resources and agents/roles that are excluded from the scope. We already excluded the *Service Provider* and *Energy Manager* from the scope of the ISMS. The template in Tab. 2 states the reasoning behind these decisions. We consider assets, which are also part of the scope of an ISMS, in the following part of our method.

**Table 1.** Instantiated Template for Locations of ISMS Elements

| **Si* Element** | **Location** |
|---|---|
| power plant | Hannover, Germany |
| ... | ... |

**Table 2.** Instantiated Template for Locations of ISMS Elements

| **Si* Element** | **Reason for Scope Exclusion** |
|---|---|
| Energy Manager | The Energy Manager has already an ISO 27001 compliant ISMS in place. |
| Service Provider | The Service Provider offers software of different kinds to the Consumer. It is assumed that the Service Provider certifies all services compliant to the Common Criteria [5]. |
| ... | ... |

**Step 3: Identify Assets -** The design goal of the ISO 27001 ISMS is to protect assets with adequate security controls and this is stated already on page 1 of the standard. Section 4.2.1 a of the standard demands the definition of assets. Section 4.2.1 b concerns the definition of ISMS security policies and it demands that the policy shall consider assets. Section 4.2.1 d that concerns risk identification uses the scope definition to identify assets, to analyse threats to assets, and to analyse the impacts of losses to these assets. Section 4.2.1 e concerns risk analysis, which also clearly define to analyse assets and to conduct a vulnerability analysis regarding assets in light of the controls currently implemented. Thus, identification and analysis of assets is a vital part of establishing an ISO 27001 compliant ISMS. An asset is defined in the standard as "anything that has value to the organisation" [1, p. 2]. We propose the following steps for identifying assets, which concern resources in our SI* model. Thus, the following step aims to find resources and if the resources have a value for the asset owner, they are assets.

**Investigate the Eco Model Relations.** The relations of the *Eco Model*: *request*, *own*, and *provide* that consider a resource at one end reveal possible assets and in case of the *own* relation, also the asset owner.

**Investigate Goal Relations.** Means-end relations between a goal and a resource have to be investigated. In addition, for each goal we have to check if not a resource is missing that might be an asset.

**Iterate over all Resources.** In order not to miss any assets, an iteration of all resources in the model is done and a check is conducted if this is an asset.

For an accurate description of assets the following information has to be elicited for each asset.

**State the Asset Owner.** Check if the *own* relation of the Eco Model is set on an asset. If this is the case, the agent or role on that relation is the asset owner. If this relation is not set, it has to be included into the model.

**Define the Need of Protection.** We want to state the need for protection of an asset. This information can help to assess an initial risk level for an asset and serves as an input of the threat analysis. At this stage only the trust relations in the SI* model are considered. Any assets (resources) that have an *execution dependency* or *permission delegation* relation have an interaction with another agent or role. These can require a need of protection, which has to be described. The trust relations *trust of execution* or *trusting in execution* result in a limited need for protection, while a *distrust relation* requires a significant protection.

**Assess Initial Risk.** The description of assets and their need for protection entries shall be analysed by domain experts and initial risk values shall be assigned. These values are meant to categorise assets by risk level. We propose to limit the possible labels to low (1), medium (2), and high (3) as proposed by the NIST 800-30 [6] standard for risk management. These values are later in the process refined in order to assess if an asset has an acceptable risk level in light of its threats or if additional controls are needed. We illustrate the resulting asset list in Tab. 3.

**Table 3.** Asset List

| **Asset** | **Asset Owner** | **Need for Protection** | **Risk Level** |
|---|---|---|---|
| Power Plant | Energy Provider | The power plant produces the energy sold and consumed in the smart grid. Its availability is of utmost importance. | 3 |
| ... | ... | ... | ... |

**Step 4: Analyze Threats -** The ISO 27001 standard concerns threat analysis in several sections for determining the risks to assets. Section 4.2.1 d demands a threat analysis for assets for the purpose of identifying risks and the vulnerabilities that might be exploited by those threats. Section 4.2.1 e concerns risk analysis and evaluation and demands to determine likelihoods and consequences for threats.

The ISO 27001 standard demands threat analysis in order to determine and analyse risks to assets. In particular, the standard mentions the importance of physical and network threat analysis. We consider four basic kinds of attackers for our threat analysis as proposed in [7]. These are *software attackers* that target software systems, *network attackers* that are reading or manipulating network traffic, *physical attackers* that are targeting hardware installations, and *social engineering attackers* that manipulate roles or agents. A study of the SANS Institute from 2006[4] revealed four fundamental motivations of social engineering attackers: Financial gain, self-interest, revenge, external pressure. We believe these motivations are generic enough to serve all types of IT attackers. We also added the motivation curiosity, which we identified in discussions with the industrial partners of the NESSoS project. We explain all of these motivations in the following: We model attacker motivations as soft goals of attackers, depicted in Fig. 2. The assumptions about each attacker are annotated using UML notes. The refined goals of attackers from their soft goals are threats. This refinement is modeled with *means-end* relationships, because the threats are a means to act upon the attacker's motivation. We use the *means-end* relationship to model relations between threats and resources, as well. The reason is that the exploit of a resource fulfills a threat. For simplicity's sake, we show only the elements of the SI* model necessary for the threat analysis in Fig. 2.

We consider two different *Network Attacker*s in our analysis. One *Network Attacker* has the soft goal *External Pressure*. Hence, the *Network Attacker* has the capabilities to attack the network, but no motivation for doing so. We assume the attacker is pressured by a criminal organisation to *Access and Manipulate Network Traffic*. The resources this goal targets are the *Security Module*, the *Smart Meter*, and the *Gateway to the Grid*, because all of these are connected via a network and we assume the *Network Attacker*

[4] `http://www.sans.org/reading_room/whitepapers/engineering/social-engineering-means-violate-computer-system_529`

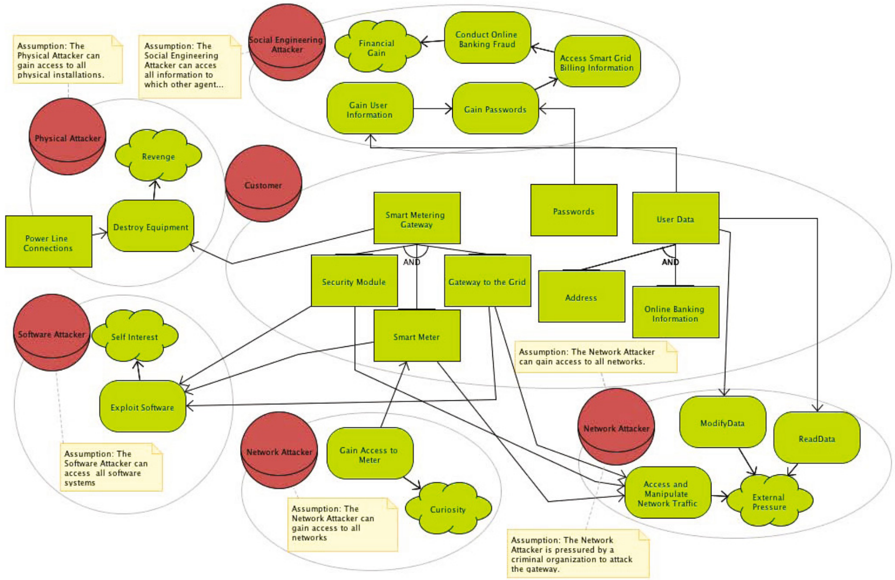
Assumption: The Physical Attacker can gain access to all physical installations.
Assumption: The Social Engineering Attacker can acces all information to which other agent...
Social Engineering Attacker
Financial Gain
Conduct Online Banking Fraud
Access Smart Grid Billing Information
Gain User Information
Gain Passwords
Physical Attacker
Revenge
Customer
Power Line Connections
Destroy Equipment
Smart Metering Gateway
Passwords
User Data
AND
Security Module
Gateway to the Grid
Address
AND
Online Banking Information
Software Attacker
Self Interest
Smart Meter
Assumption: The Network Attacker can gain access to all networks.
Exploit Software
Network Attacker
ModifyData
ReadData
Assumption: The Software Attacker can access all software systems
Network Attacker
Gain Access to Meter
Access and Manipulate Network Traffic
External Pressure
Curiosity
Assumption: The Network Attacker can gain access to all networks
Assumption: The Network Attacker is pressured by a criminal organization to attack the gateway.

**Fig. 2.** SI* Diagram concerning goal-based Threat Analysis

can gain access to all networks. The *Network Attacker* is pressured to *Read Data* and *ModifyData*. *User Data* is *owned* by the customer and threatened by the *Network Attacker*, as well. These threats are a means to achieve the goals of the *Network Attacker*. A second *Network Attacker* acts out of *Curiosity* and gains access to the *Smart Meter*. The *Social Engineering Attacker* has the soft goal to get *Financial Gain* from attacking the *Smart Metering Gateway*. The attacker wants to *Conduct Online Banking Fraud* and for this purpose *Access the Smart Grid Billing Information*. The attacker aims to *Gain Passwords* of the *Consumer*. After the attacker has acquired the *Passwords* of the *Consumer*, the attacker can *Gain User Information*. The *Physical Attacker* is motivated by *Revenge* against the *Customer* and wants to *Destroy Equipment*. The attacker targets the *Power Line Connections* and the *Smart Metering Gateway*. The *Software Attacker* is motivated by *Self Interest* and wants to *Exploit Software* in order to hide data about his or her energy consumption. For simplicity's sake we do not show all possible attackers and their motivations. However, we show exemplary the exclusion of one attacker. The *Physical Attacker* with the motivation *Financial Gain* is not considered, because the effort and skill required to steal a *Smart Metering Gateway* is not worth the insignificant monetary value for it. In particular, because the *Energy Manager* has equipped the gateway with IDs and the *Energy Manager* can block the access of stolen gateways to the smart grid. We use the elicited threats as inputs for misuse cases [4]. These are textual representations of attacker's actions for threat identification. We use them to derive security requirements and check for missing threats. We propose a table as introduced by Deng et al. [8] that lists misuse cases and their corresponding security requirement.

**Table 4.** From Misuse Cases to Security Requirements

| Misuse Case | Security Requirement |
|---|---|
| 1. The confidentiality of the *Consumer*'s *Passwords* might be compromised by a *Social Engineering Attacker*. | Ensure that the confidentiality of the *Passwords* is not compromised by a social engineering attack. |
| 2. The availability and integrity of the *Smart Metering Gateway* can be compromised by a *Software Attacker*. | The *Smart Metering Gateway* has to be protected against *Software Attackers* that aim to execute exploits. |
| ... | ... |

In contrast to the work of Deng et al., we do not consider solutions in this step. We discuss these during the selection of ISO 27001 security controls in the following. We illustrate several misuse cases in Tab. 4.

**Step 5: Conduct Risk Assessment and Control Selection -** Risk management is mentioned in numerous sections of the ISO 27001 standard. In the method risk is used to assess if an asset requires an additional control or not. We use the risk management technique proposed by Asnar et al. [9] for goal-based requirements engineering. For simplicity's sake, we do not explain it in detail in this work.

For each of the assets that has an unacceptable risk level controls have to be selected to reduce that risk. We use the resulting security requirements of the threat analysis as guidance for selecting controls. The numbering of the controls starts with A.5 and ends with A.15. The reason for not starting the numbering with A.1 is that the control numbering shall align with the controls listed in the ISO/IEC 17799:2005 standard. This standard provides guidelines on how to implement the controls, but it is not normative.

For the requirement 2 from Tab. 4 we choose adequate controls. The control *A.10 Communications and operations management* contains the sub control *A.10.4 Protection against malicious and mobile code*. Further sub controls are *A.10.4.1 Controls against malicious code*, which is described as "Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented. "[1, p. 19]. In addition, another relevant sub control is *A.10.4.2 Controls against mobile code*: "Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing." [1, p. 19]. The selection of these controls is followed by selecting concrete measures. For example, we have to conduct penetration testing in order to find existing vulnerabilities in the software of the *Smart Metering Gateway* and fix these. For each asset, we have to iterate over all controls in the Appendix A of the ISO 27001 standard and state if a control is required or not for that asset. The resulting document is the so-called *Statement of Applicability*.

**Step 6: Design ISMS Specification -** The ISO 27001 standard demands a documentation of the ISMS. The standard demands several documents for each part of the ISMS, but the standard states no demands for the form or medium. Hence, we developed a mapping (see Tab. 5) of the generated artifacts from our method to the documentation demands.

**Table 5.** Support of our Method for ISO 27001 Documentation Demands

| ISO 27001 Documentation Requirement | Artifacts of our Methods |
|---|---|
| ISMS policies and objectives | Misuse cases and Security Requirements |
| Scope and boundaries of the ISMS | SI* diagrams |
| Procedures and controls | Documentation of selected security controls and their implementation |
| The risk assessment methodology | Description of the method by Asnar et al. [9] |
| Risk assessment report | Results of asset identification and threat analysis including SI* models |
| Risk treatment plan | Risk Assessment and Control Selection |
| Information security procedures | Control Documentation of resulting security processes |
| Control and protection of records | Documentation of selected measures to control documents |
| Statement of Applicability | Reasoning about Controls |

## 6 Discussion and Related Work

The procedure presented in this chapter was developed based on discussions with practitioners from security and especially ISO 27001 projects. Parts of our method was discussed with security consultants. The security consultants mentioned that this structured procedure

- Helps to describe the attackers' abilities in more detail,
- Supports the identification of all threats on the given assets,
- Supports the identification and classification of assets.
- Increases the use of models instead of texts in standards, which eases the effort of understanding the system documentation,
- Provides the means for abstraction of a complex system and structured reasoning for security based upon this abstraction.

One issue that needs further investigation is that of scalability, both in terms of the effort needed by the requirements engineer in order to enter all information about the organization and the threat analysis proposed. We will use the method for different scenarios to investigate if the method scales for complex goal models.

To the best of our knowledge no approach exist to use a goal-based security requirements engineering approach for ISO 27001 complaint ISMS establishment.

Mellado et al. [10] created the Security Requirements Engineering Process (SREP). SREP is an iterative and incremental security requirements engineering process. In addition, SREP is asset-based, risk driven, and follows the structure of the Common Criteria [11]. The work differs from ours, because the authors do not support the ISO 27001 standard.

## 7 Conclusion

We have presented a structured method to establish an Information Security Management System (ISMS) according to the ISO 27001 standard, which builds upon the security requirements engineering method SI*. Our method provides the means to elicit the context of an ISMS consider management commitment, threat and risk analysis, as well as security requirements-based control selection.

Our method offers the following main benefits:

- A structured method for describing the context, analyzing threats and risks, formulating security requirements, and selecting ISO 27001 controls,
- Re-using SRE methods to support the development of an ISO 27001 ISMS,
- Support for generating consistent ISMS documentation compliant to ISO 27001
- Re-using the structured techniques of SRE methods for analyzing complex systems and eliciting security requirements, to support the refinement of sparsely described sections of the ISO 27001 standard.

## References

1. 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)
2. Massacci, F., Mylopoulos, J., Zannone, N.: Security requirements engineering: The SI* modeling language and the secure tropos methodology. In: Ras, Z.W., Tsay, L.-S. (eds.) Advances in Intelligent Information Systems. SCI, vol. 265, pp. 147–174. Springer, Heidelberg (2010)
3. Beckers, K., Faßbender, S., Heisel, M., Küster, J.-C., Schmidt, H.: Supporting the Development and Documentation of ISO 27001 Information Security Management Systems through Security Requirements Engineering Approaches. In: Barthe, G., Livshits, B., Scandariato, R. (eds.) ESSoS 2012. LNCS, vol. 7159, pp. 14–21. Springer, Heidelberg (2012)
4. Opdahl, A.L., Sindre, G.: Experimental comparison of attack trees and misuse cases for security threat identification. Inf. Softw. Technol. 51, 916–932 (2009)
5. ISO and IEC: Common Criteria for Information Technology Security Evaluation. ISO/IEC 15408, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2009)
6. Stoneburner, G., Goguen, A., Feringa, A.: Risk management guide for information technology systems. NIST Special Publication 800-30, National Institute of Standards and Technology (NIST) (2002)
7. Beckers, K., Côté, I., Hatebur, D., Faßbender, S., Heisel, M.: Common Criteria CompliAnt Software Development (CC-CASD). In: Proceedings 28th Symposium on Applied Computing, pp. 937–943. ACM (2013)
8. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requir. Eng. 16, 3–32 (2011)
9. Asnar, Y., Giorgini, P., Massacci, F., Zannone, N.: From trust to dependability through risk analysis. In: Proceedings of ARES, pp. 19–26 (2007)
10. Mellado, D., Fernandez-Medina, E., Piattini, M.: A comparison of the common criteria with proposals of information systems security requirements. In: ARES, pp. 654–661 (April 2006)
11. Mellado, D., Fernández-Medina, E., Piattini, M.: Applying a security requirements engineering process. In: Gollmann, D., Meier, J., Sabelfeld, A. (eds.) ESORICS 2006. LNCS, vol. 4189, pp. 192–206. Springer, Heidelberg (2006)