ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System

Kristian Beckers[1], Maritta Heisel[1], Bjørnar Solhaug[2], and Ketil Stølen[2,3]

[1] Paluno, University of Duisburg-Essen, Germany
[2] SINTEF ICT, Norway
[3] Dep. of Informatics, University of Oslo, Norway
{kristian.beckers,maritta.heisel}@paluno.uni-due.de,
{bjornar.solhaug,ketil.stolen}@sintef.no

Abstract. Established standards on security and risk management provide guidelines and advice to organizations and other stakeholders on how to fulfill their security needs. However, realizing and ensuring compliance with such standards may be challenging. This is partly because the descriptions are very generic and have to be refined and interpreted by security experts, and partly because they lack techniques and practical guidelines. In previous work we showed how existing security requirements engineering methods can be used to support the ISO 27001 information security standard. In this chapter we present ISMS-CORAS, which is an extension of the CORAS method for risk management that supports the ISO 27001 standard. ISMS-CORAS comes with techniques and guidelines necessary for establishing an Information Security Management System (ISMS) compliance with the standard, as well as the artifacts that are needed for the required documentation. We validate the method by applying it to a scenario from the smart grid domain.

Keywords: Information security, risk analysis, security standard compliance, ISO 27001, CORAS.

1 Introduction

The management of security and risk, as well as identifying and fulfilling the security needs, is challenging for many organizations and other stakeholders. Fortunately, several security standards, such as ISO 27001 [19], offer ways to attain this goal in a structured and systematic way. The mentioned standard prescribes a process for establishing and maintaining an Information Security Management System (ISMS), which tailors security to the specific needs of any kind of organization. However, several ambiguities in the standard need to be handled, and the organizations need to understand and decide how to operationalize the standard, and how to document the ISMS.

This security standard is ambiguous on purpose, because it should serve a multitude of different domains and stakeholders. The ambiguity is nevertheless

M. Heisel et al. (Eds.): Engineering Secure Future Internet Services, LNCS 8431, pp. 315–344, 2014.

a problem for the stakeholders who have to choose a method for security analysis that is compliant with the standard. The stakeholders moreover need to decide the abstraction level for the required documentation without any support from the standard. For example, security experts have to describe the business, processes, actors and roles, technologies, etc., and decide on their own what is the most relevant scope elements to consider. In addition, the security experts have to find a method that allows them to achieve completeness of identifying stakeholders, security objectives, assets and other elements within the desired scope. Moreover, the standard does not provide any techniques or methods for assembling the necessary information, or a pattern or template for structuring and documenting this information. The importance of these steps becomes apparent when one realizes that essential further steps of ISO 27001 depend upon them, including the identification of threats, vulnerabilities and security controls.

In this chapter we propose an extension of the CORAS method [28] to support the establishment of an ISO 27001 compliant ISMS. In previous work we analyzed the relations between different security requirements engineering and risk analysis methods [7], and our results showed that the ISO 27001 standard has a significant focus on risk analysis. It describes how to build an ISMS, and CORAS already supports many of these steps due to its focus on risk management. A further motivation for building on CORAS is that the method is based on the ISO 31000 [18] risk management standard, which is also the basis for the information security risk management process of ISO 27005 [20]. The latter standard refines the risk management process described in the ISO 27001.

In addition, the ISO 27001 standard demands legal aspects (such as laws, regulations, contracts and legally binding agreements) to be considered. CORAS provides support for this during the risk analysis by an extension called *Legal CORAS* [28]. CORAS also comes with tool and modeling support for all phases of the process. The approach moreover facilitates the reporting of the results by a formal mapping of its diagrams to English prose, which is useful for generating the documentation that is required by ISO 27001.

In summary, we use CORAS as a basis because of its structured method for risk management, its compliance to ISO 31000, the consideration of legal aspects, the tool support and the support for document generation. The CORAS approach has moreover undergone thorough industrial validation in many different domains over more than a decade [28].

We refer to the CORAS extension presented in this report as *ISMS-CORAS*. We show how we extend CORAS, and we present a mapping from the resulting ISMS-CORAS artifacts to the ISMS documentation compliant with ISO 27001. We apply our method to a smart grid scenario provided by the industrial partners of the NESSoS project [35].

Compared to standard CORAS, which is a method for risk analysis in general, there are a number of novel features and artifacts of ISMS-CORAS. First of all, ISMS-CORAS comes with diagrams and templates to support all documentation requirements of the ISO 27001 standard. This documentation support goes well beyond the modeling support of CORAS. It moreover comes with a classification of attacker types, templates for attacker description, and attacker overview diagrams to facilitate the attacker identification. It has support for identification of attacker motivation and entry points, and for modeling this information in the threat diagrams. These and other novelties in combination provide a systematic support for establishing and documenting an ISMS in compliance with the standard.

The outline of this chapter is as follows. In Section 2 we describe the background to ISMS-CORAS, and in Section 3 we describe the method, the documentation artifacts and how ISMS-CORAS supports the ISO standard. In Section 4 we demonstrate and exemplify ISMS-CORAS by using the smart grid scenario. The section also describes in more details the documentation artifacts introduced in Section 3. Related work is presented in Section 5 before we conclude in Section 6.

The presentation of ISMS-CORAS in this chapter is a shortened version of a technical report with the same title [10]. We refer the reader to the report for the full description of ISMS-CORAS and for a more detailed description of all the documentation artifacts. The report also gives more detailed references to the ISO 27001 demands, as well as a more elaborated presentation of the application of ISMS-CORAS to the smart grid scenario.

The security and risk terminology that we use in this chapter is based on both CORAS and the above mentioned standards. The technical report comes with an appendix with a comparison of the respective terminologies and a clarification of the underlying terminology of ISMS-CORAS.

2 Background

In this section we briefly describe the main background to the ISMS-CORAS method, namely the CORAS method and its extension Legal CORAS [28], as well as the ISO 27001 standard [19].

2.1 CORAS

CORAS is a model-driven approach to risk analysis that follows the process defined by the ISO 31000 risk management standard [18]. The approach consists of three tightly integrated artifacts, namely the CORAS method, the CORAS language and the CORAS tool. The method comes with techniques and practical guidelines, and the language provides modeling and documentation support for all steps of the method. The tool is a diagram editor for creating any CORAS diagram. The overall process consists of the five following consecutive steps, which is also according to ISO 31000.

Establishing the context involves setting the scope and focus of the analysis, identifying the assets with respect to which risks are identified, and defining the risk evaluation criteria. The target of analysis is specified at the desired level of abstraction using a precise and well-understood notation, such as UML [36]. The documentation of the context establishment is used as input to and a basis for the subsequent risk assessment.

The risk assessment includes the three steps of *risk identification*, *risk estimation* and *risk evaluation*. Risk identification is to identify and document unwanted incidents, together with the threats and vulnerabilities that may cause them, using CORAS threat diagrams. The risk estimation involves the estimation of likelihoods and consequences for the unwanted incidents using the threat diagrams. In order to facilitate the risk estimation and to identify the most important sources of risk, likelihoods are estimated also for threats and threat scenarios. The results of the risk estimation are documented using CORAS *risk diagrams*. The risk evaluation involves comparing the identified risks with the risk evaluation criteria, and to determine which risks are unacceptable. In addition to structured brainstorming, a technique for risk identification and estimation that brings together people with different expert insight into the target of analysis, CORAS makes use of any other input such as statistics, security logs, questionnaires, and so forth.

Finally, the *risk treatment* is to identify means for mitigating unacceptable risks. This is also conducted by structured brainstorming, and is supported by CORAS *treatment diagrams*.

2.2 Legal CORAS

Legal CORAS is an extension of CORAS specifically for considering legal aspects and legal risk. The method elicits relevant legal aspects based on the target of analysis and the target description.

The source of legal risk is legal norms, which are norms that stem from a legal source such as laws, regulations, contracts and legally binding agreements. When assessing legal risk, there are two kinds of uncertainties that must be estimated. First, the legal uncertainty is the uncertainty of whether a specific norm actually applies to circumstances that may arise. Second, the factual uncertainty is the uncertainty of whether the circumstances will actually occur, and thereby potentially trigger the legal norm. It is by combining the estimates for these two notions of uncertainty that we can estimate the significance of a legal norm and its impact on the risk picture. Legal CORAS comes with the necessary analysis techniques and modeling support, but the involvement of a lawyer or other legal experts is usually required.

2.3 ISO 27001

The ISO 27001 standard is structured according to the Plan-Do-Check-Act (PDCA) model, which is referred to as the ISO 27001 process. 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.

We focus in our work on the Plan phase, because we provide a specific method for building an ISMS, and because it is during this phase that the security risk analysis is stressed the most. In future work we will also develop support for the other phases of the PDCA model.

Table 1. ISO 27001 documentation demands

#	**Name**
1.	The scope of the ISMS
2.	The ISMS policy statements that contain general directions towards security and risk
3.	Procedures and controls in support of the ISMS
4.	A description of the applied risk assessment methodology
5.	A risk assessment report
6.	A risk treatment plan
7.	Documented procedures to the effective planning, operation and control of the ISMS
8.	ISMS records
9.	Statement of applicability
10.	Management decisions

The Plan phase considers the scope and boundaries of the ISMS, its interested parties, the environment, and the assets. All the technologies involved are moreover defined, as well as the ISMS policies, risk assessments, evaluations, and controls. Controls in the ISO 27001 are measures to modify risk.

The ISO 27001 standard demands a set of documents for certification, which we introduce in Table 1. Note that the names of the ten documents are given by us to simplify the reference to them when presenting ISMS-CORAS throughout this chapter. The standard itself describes these documents only by their contents.

Document 8, the ISMS records, is for providing evidence of compliance to the requirements of the ISMS. This is out of the scope of ISMS-CORAS, which rather concerns the establishment of the ISMS, and is therefore not among the ISMS-CORAS documentation artifacts. ISMS-CORAS is also not providing document 4, since the risk assessment method is part of ISMS-CORAS itself. Document 9 is for describing the control objectives and controls that are relevant and applicable to the organization's ISMS, whereas document 10 provides support for establishing and maintaining an ISMS.

3 The ISMS-CORAS Method

The ISMS-CORAS method is conducted according to the five steps depicted to the left in Figure 1. These consecutive steps comprise the risk analysis process as defined by the ISO 31000 risk management standard that also CORAS complies with. ISMS-CORAS is defined as an extension of CORAS, and while keeping the names of the steps we focus in our description of ISMS-CORAS on the novel artifacts and the changes with respect to standard CORAS. We explain how our changes to CORAS are related to ISO 27001 and its documentation requirements as described in the previous section. The reader is referred to existing literature for details about standard CORAS [28].

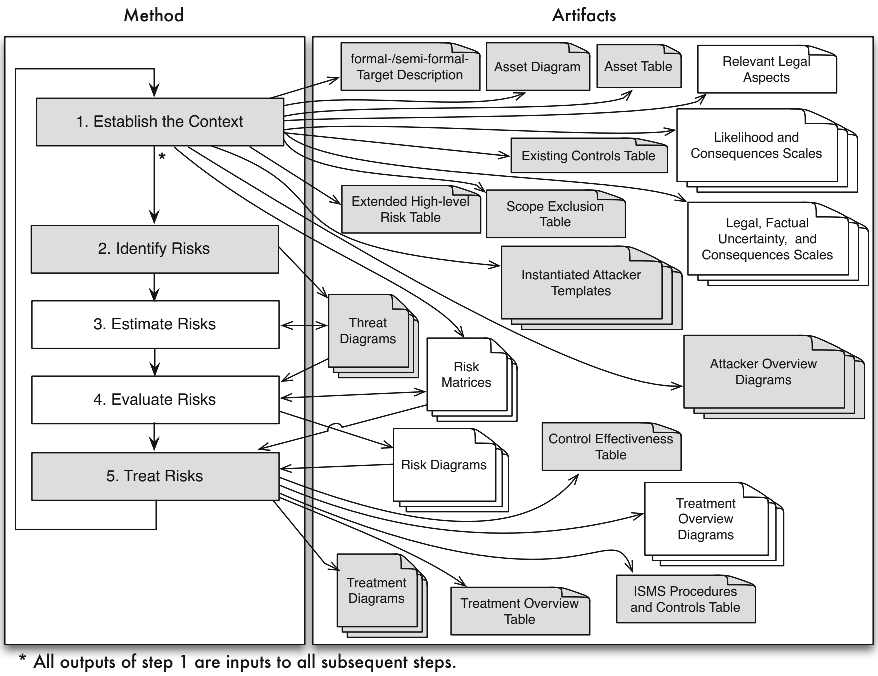
Method
Artifacts
1. Establish the Context
*
2. Identify Risks
3. Estimate Risks
4. Evaluate Risks
5. Treat Risks
formal-/semi-formal-Target Description
Asset Diagram
Asset Table
Relevant Legal Aspects
Likelihood and Consequences Scales
Existing Controls Table
Extended High-level Risk Table
Scope Exclusion Table
Legal, Factual Uncertainty, and Consequences Scales
Instantiated Attacker Templates
Threat Diagrams
Risk Matrices
Attacker Overview Diagrams
Control Effectiveness Table
Risk Diagrams
Treatment Overview Diagrams
Treatment Diagrams
Treatment Overview Table
ISMS Procedures and Controls Table
* All outputs of step 1 are inputs to all subsequent steps.

Fig. 1. ISMS-CORAS method and artifacts

The CORAS steps that we have modified are depicted in grey in Figure 1. The same is the case for the novel or modified documentation artifacts as depicted to the right. Note that the ISO 27001 standard does not have specific demands on the form of the documentation, as “documents and records may be in any form or type of medium” [19]. When introducing the ISMS-CORAS method in this section we explain the steps and tasks, as well as the documentation artifacts that are produced and used. We refer to Section 4 for examples of the artifacts.

Also note that in addition to the ISMS-CORAS documentation artifacts, the results should be documented by accompanying prose and textual documents. The main purpose of the artifacts is to support the method, structure the results in adequate ways, and ensure completeness of fulfilling the tasks and requirements of the ISO standard.

3.1 Step 1: Establish the Context

The first step of ISMS-CORAS is to establish the context of the ISMS. The main objective of this step is as for CORAS, namely to build the target description and to set the scope and focus of the analysis. There are, however, several extensions that are needed in order to fulfill the standard. We have also developed additional support for increasing the focus on information security as compared to CORAS, thereby facilitating the subsequent risk identification and threat modeling. Due to the extensions we have structured Step 1 of ISMS-CORAS into five sub-steps.

Step 1.1: Develop the Target Description. This task is to build the description of the target of analysis, including the relevant actors, roles, components, work processes, business processes, networks, etc. The description should include all parts of the system or organization that are included in the analysis and governed by the ISMS. It will serve as part of the basis of the subsequent risk identification and estimation, and it is therefore important that the level of abstraction reflects the desired level of details for the security risk analysis.

ISMS-CORAS requires an explicit description of the geographical location of the elements in the target description due to demands in the ISO 27001 standard. Such location information may also be important for the required identification of relevant legal issues. For example, according to the German Federal Data Protection Act, it is not allowed to store personal information outside of the European Union.

As for CORAS, ISMS-CORAS does not require a specific notation or language to be used for creating the target description. This is the decision of the customer and/or the risk analysts, but the description should be sufficiently precise or formal to avoid ambiguities and misunderstandings. Notations like UML [36] or similar are recommended.

A task that is specific for ISMS-CORAS is the justification of any exclusions from the scope of the ISMS. This is documented in a scope exclusion table that refers to target elements and provides the reason for the exclusion.

Step 1.2: Specify Security Objectives and Assets. The identification of the security objectives and the assets is an essential step in defining the focus of the analysis. CORAS is asset-driven, which means that all activities of the risk assessment are targeting these assets, which means that threats and vulnerabilities that are irrelevant for the identified assets are disregarded. The related task of characterizing the security objectives is required by the ISO standard.

The security objectives concern the protection of information security properties such as confidentiality, integrity and availability. An asset is anything of value to the organization for which the ISMS is established, and ISMS-CORAS focuses on information assets related to the target of analysis and the identified security objectives. The identified assets are documented using CORAS asset diagrams. ISMS-CORAS moreover requires a prioritization of assets, as well as the assignment of an asset owner to each asset, both of which are documented in an asset table. According to the ISO standard, the asset owner is the individual or entity responsible for the asset and its security, and is not an assignment of property right.

ISMS-CORAS requires also the documentation of existing controls for each of the identified assets using a table format. This is a detailing of the target description, and facilitates both the risk identification and the identification of any further necessary controls.

Step 1.3: Conduct High-Level Security Risk Analysis. In addition to the specification of the target of the analysis and the asset identification, CORAS recommends conducting a high-level risk analysis in order to identify the main concerns. ISMS-CORAS extends this activity with tasks specifically related to the security objectives and the preservation of security properties. For this purpose ISMS-CORAS provides three documentation artifacts, namely attacker templates, attacker overview diagrams and a high-level risk table.

The attacker template is a table format for describing attacker types, the assets and security properties they may threaten, the attack entry points and paths, attacker skills and motivation, as well as further relevant information. The instantiation of these templates not only serves as a basis for the subsequent and more detailed risk identification; it also documents attackers that are excluded from the scope, including the justification. This will help focusing the risk analysis, and also facilitate future maintenance and management of the ISMS, in particular when there are any changes in the organization or in the security objectives.

An attacker overview diagram is a graphical and high-level representation of an instantiated attacker template. It gives an intuitive representation of the identified attackers, and is a useful means for checking completeness of the attacker description.

The high-level risk analysis is an initial identification of scenarios and incidents that can be caused by the attackers, the vulnerabilities that may be exploited, as well as the related security objectives. The results are documented in the high-level risk table which serves as a basis for structuring the risk identification.

Step 1.4: Define the Scales and the Risk Evaluation Criteria. This task is similar to CORAS and most other approaches to risk analysis. It involves defining the scales that are needed for estimating the risks, as well as developing the criteria for accepting risks.

Risks are estimated by estimating the likelihoods and consequences of unwanted incidents. Hence, the scales to be defined are for making and documenting these estimates. Both likelihoods and consequences can be specified quantitatively or qualitatively, and we can use intervals or continuous scales. ISMS-CORAS uses the risk matrix format for specifying the risk level of each combination of a likelihood and a consequence, and for defining the risk evaluation criteria.

Step 1.5: Identify Legal Aspects. All relevant legal issues must be considered during the context establishment of the ISMS-CORAS method due to requirements of the ISO 27001 standard. The identification of legal aspects can be achieved by using our law pattern method [8,14], methods for legal risk management [30], or by involving lawyers or other domain experts.

While taking legal aspects into account, the focus of ISMS-CORAS is still on information security. Hence, the legal aspects to consider are mostly those that can arise due to information related issues such as privacy and data protection.

However, it may also be related to other laws and regulations, and to contractual obligations or legally binding agreements.

ISMS-CORAS makes use of Legal CORAS where legal norms that may cause risks are identified and analyzed. This requires the specification of scales for estimating legal uncertainty.

Further Considerations. In addition to the five sub-steps of the context establishment, Step 1 of ISMS-CORAS cannot be concluded until a written management and resource commitment for the ISMS has been provided as demanded by the ISO 27001 standard. ISMS-CORAS moreover requires the decision makers to formally approve the documentation of the context establishment.

The standard finally requires the identification of risk assessment methodology that will be applied when establishing the ISMS. In our case, the method is ISMS-CORAS as it has been developed for conducting security risk assessment compliant with the standard.

3.2 Step 2: Identify Risks

The objective of this step is to identify the risks that must be managed by determining where, when, why and how they may occur. The risk identification is conducted by a systematic walkthrough of the target description in order to identify incidents that may arise with respect to the identified assets. Following CORAS, the risk identification may be conducted by structured brainstorming involving people from different backgrounds and with different expert insight into the target of analysis. The task may also be supported by historical data, statistics, available repositories and databases of known threats and vulnerabilities, etc.

The risk identification is supported by CORAS threat diagrams, which are designed to support on-the-fly risk modeling during brainstorming sessions. The diagrams moreover document the results of this step. In particular, threat diagrams model how threats may exploit vulnerabilities in order to cause threat scenarios that lead to unwanted incidents.

ISMS-CORAS makes use of the instantiated attacker templates and attacker overview diagrams from Step 1. The resulting threat diagrams are therefore refinements of the initial attacker descriptions and the high-level risk analysis. ISMS-CORAS moreover extends the CORAS threat diagram notation with support for specifying attacker types and relating elements of the threat diagram to the models from the target description. ISMS-CORAS also makes use of Legal CORAS to make legal aspects explicit in the analysis and in the threat diagrams.

3.3 Step 3: Estimate Risks

The objective of this step is to estimate the identified risks by estimating the likelihoods and consequences of the identified unwanted incidents. CORAS makes use of structured brainstorming and any available data also for this task, and the results are documented by annotating the threat diagrams. Likelihoods of threat scenarios as well as conditional likelihoods for one scenario to lead to another are estimated in order to provide a stronger basis for the risk estimation and to understand the most important sources of risk. The CORAS calculus supports the estimation, and can also be used for consistency checking.

ISMS-CORAS focuses on the likelihoods of misuses and exploits by considering the attacker types and attacker skills documented during Step 1, which is similar to the descriptions proposed by the Common Criteria [21].

3.4 Step 4: Evaluate Risks

The objective of the risk evaluation is to determine which risks are acceptable and which risks need to be evaluated further for possible treatment. The step is identical to CORAS, and involves using the risk evaluation criteria from Step 1 together with the results from the risk estimation.

3.5 Step 5: Treat Risk

The objective of this step is to identify cost-effective means to mitigate unacceptable risks by reducing the likelihood and/or the consequence of unwanted incidents. CORAS uses treatment diagrams for this tasks, where identified treatments are related to the risk elements that are treated. ISMS-CORAS extends the notation by relating treatments to the relevant part of the target of analysis.

A further requirement of ISMS-CORAS is that the treatment identification is restricted to the normative controls defined in Appendix A of ISO 27001. Additional support for treatment identification is provided by a mapping from the ISMS-CORAS attacker types to ISO 27001 controls. This mapping includes a description of the objective of each control, as well as the kinds of target elements that are relevant.

As part of the risk treatment step, the existing controls must be taken into account, and treatment responsibility assigned to the asset owner. The residual risks must be documented and approved by the management. The treatment plan should be made by use of cost-benefit reasoning, for example by using the CORAS extension we proposed in earlier work [46].

ISMS-CORAS moreover requires the justification for why any Appendix A control is left out. For this purpose the treatment documentation incudes filling out a treatment overview table. For each treatment, this table specifies the related asset, asset owner and security objective, as well as a reasoning of why the treatment is sufficient. A control exclusion table specifies for each Appendix A control the reason for excluding each control that is not considered.

A further demand is the documentation of how to measure the effectiveness of each control, which is supported in ISMS-CORAS by a control effectiveness measure table. Finally, an analysis of possible conflicts between the identified treatments on the one hand and legal, regulatory and contractual requirements on the other hand must be identified. For this purpose Legal CORAS can be applied.

The identified controls, the existing controls and the justification of excluded controls form the documentation that is required by the ISO standard to make the so-called statement of applicability.

3.6 Contribution to ISMS Documents

In Table 2 we give an overview of how the ISMS-CORAS documentation artifacts depicted in Figure 1 support the ISO 27001 demands on the documentation of the ISMS. The first column refers to the ISO 27001 documents listed in Table 1, the second column lists the ISMS-CORAS artifacts that provide the documentation, and the third column refers to the ISMS-CORAS method steps that produce the artifacts.

Recall from Section 2.3 that documenting the risk assessment method (document 4) and creating the ISMS records (document 8) are outside the scope of ISMS-CORAS. Note also that the ISMS-CORAS artifacts need to be accompanied with complementary written documentation whenever additional clarifications are needed. For the management decisions (document 10) such written documentation is required as there are no supporting ISMS-CORAS artifacts.

Table 2. ISMS-CORAS support for ISO 27001 documentation; the first column refers to the documents listed in Table 1

#	ISMS-CORAS artifacts	Steps
1.	Target description and model; Scope exclusion table	1
2.	High-level risk tables	1
3.	Existing controls table ISMS procedure and controls table	1, 5
4.	N/A	
5.	Asset diagrams; Asset tables; Attacker templates; Attacker overview diagrams; Likelihood and consequence scales; Risk matrices (criteria); Threat diagrams; Risk diagrams	1–4
6.	Treatment diagrams; Treatment overview diagrams;	5
7.	Treatment overview table; Control effectiveness table	5
8.	N/A	
9.	Treatment diagrams; Treatment overview table	5
10.	Prose	1,5

4 Applying the ISMS-CORAS Method to a Smart Grid Scenario

In this section we demonstrate and exemplify the use of ISMS-CORAS by applying the method to a smart grid scenario. The section also introduces in more detail the ISMS-CORAS modeling and documentation artifacts that we mentioned in the previous section. The example is a simplified and shortened presentation of the corresponding demonstration in the technical report [10].

A smart grid provides energy on demand from distributed generation stations to customers. The grid intelligently manages the behavior and actions of its participants using information and communication technology (ICT). One of the novelties as compared to existing energy networks is the two-way communication between consumers and electric power companies. The envisioned benefits of the smart grid include a more economic, sustainable and reliable supply of energy. However, significant security concerns arise due to the possible dangers of missing availability of energy for customers, as well as threats to the security of customer data. These concerns are of particular relevance for the smart grid, because energy grids have a significantly longer lifespan than telecommunication networks [4]. In addition, privacy concerns have risen due, for example, to the possibility of creating behavioral profiles of customers when their energy consumption is transmitted over the grid in small time intervals [27].

In the following we present each of the five steps of ISMS-CORAS in turn, focusing in particular on the tasks and artifacts that go beyond standard CORAS. The reader is referred to existing literature for details on the latter [28].

4.1 Step 1: Establish the Context

The context establishment includes understanding and documenting the target of analysis, setting the scope and focus, identifying the assets and security objectives, and specifying the risk evaluation criteria. We structure the presentation of this step according to the five sub-steps of this initial phase of ISMS-CORAS.

Step 1.1: Establish the Target Description. The smart grid scenario we use for the example is provided by the industrial partners of the NESSoS network of excellence [35]. It concerns a smart home, which in our example is a house that is divided into two living units of separate electricity consumers.

For the purpose of describing the target of analysis at the desired level of abstraction, we use UML class diagrams and activity diagrams. As shown in Figure 2, the class diagram includes information about geographical locations, which is demanded by ISMS-CORAS. In the following we present some of the details about two of the diagrams that we developed.

In the class diagram of Figure 2 the associations represent communication connections, as the focus of the analysis is on the communication and security of information. The elements within the indicated scope are inside the smart home, and the indicated locations are based on real smart grid experiments conducted in Germany [43].

The *ICT Gateway (ICTG)* is the connection between the smart home and the information systems of the *Energy Supplier (ES)*. The *Consumers (CO)* are the house dwellers who use *Smart Appliances (SA)*. SAs are connected to the internet via the ICTG. An SA may, for example, be a fridge that can be remotely configured to cool down to a specific temperature at a specified time. The parties can use services offered by the energy providers via a *Consumer Home Energy Display (CHED)*. A *Thermostat (TH)* measures the temperature of the home or

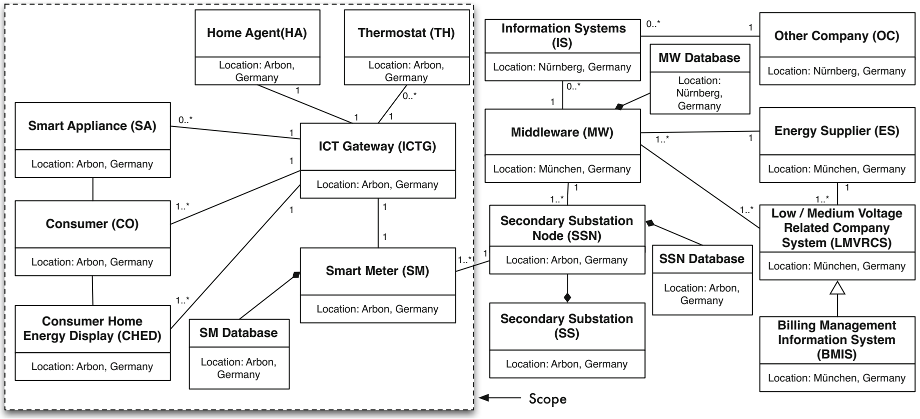

Fig. 2. Elements of the smart home scenario; the indicated scope (left part) includes the elements of the smart home, whereas the remaining elements (right part) belongs to the grid

of SAs. The temperature information is used, for example, for safety purposes, such as preventing a stove from overheating. They are also used by applications that control SAs. In addition, customers can use THs to configure SAs, for example to configure a heater to warm the smart home to a specific temperature during daytime. This information is used by the *Home Agent (HA)* to offer the CO a selection of different energy rates from different ESs [41]. Every consumer has its own *Smart Meter (SM)*, which is placed in the cellar of the smart home. The SM transfers the energy consumption/production data to the *Secondary Substation Node (SSN)*, which is part of the *Secondary Substation (SS)*.

The two consumers in this scenario share the cellar. The SM measures the energy consumption and sends the consumption information at specified intervals to the ES via the ICTG. Intermittently the energy consumption information is stored in the SM Database. Consumers can also produce energy and sell it to the ES. The SM measures this production and sends the information to the ES.

All of the communications in the smart grid are two-way and form the so-called *Advanced Metering Infrastructure (AMI)*. This scenario is in alignment with other European projects regarding smart grids [13,16,26,40].

Figure 3 shows one of the activity diagrams we specified in order to capture relevant behaviors of the target of analysis, namely the SM electricity reading for billing purposes. The SSN initiates the process every 24 hours, which is a configurable time interval. The SM receives the request, queries its internal database and sends the result back to the SSN. The process continues with some validation and verification checks before the LMVRCS eventually receives the reading. Note that we used three dots to simplify the diagram at places where activities are repeated. We refer to the technical report for the detailed description, and for the data structure model and further activity diagrams for the smart home scenario.

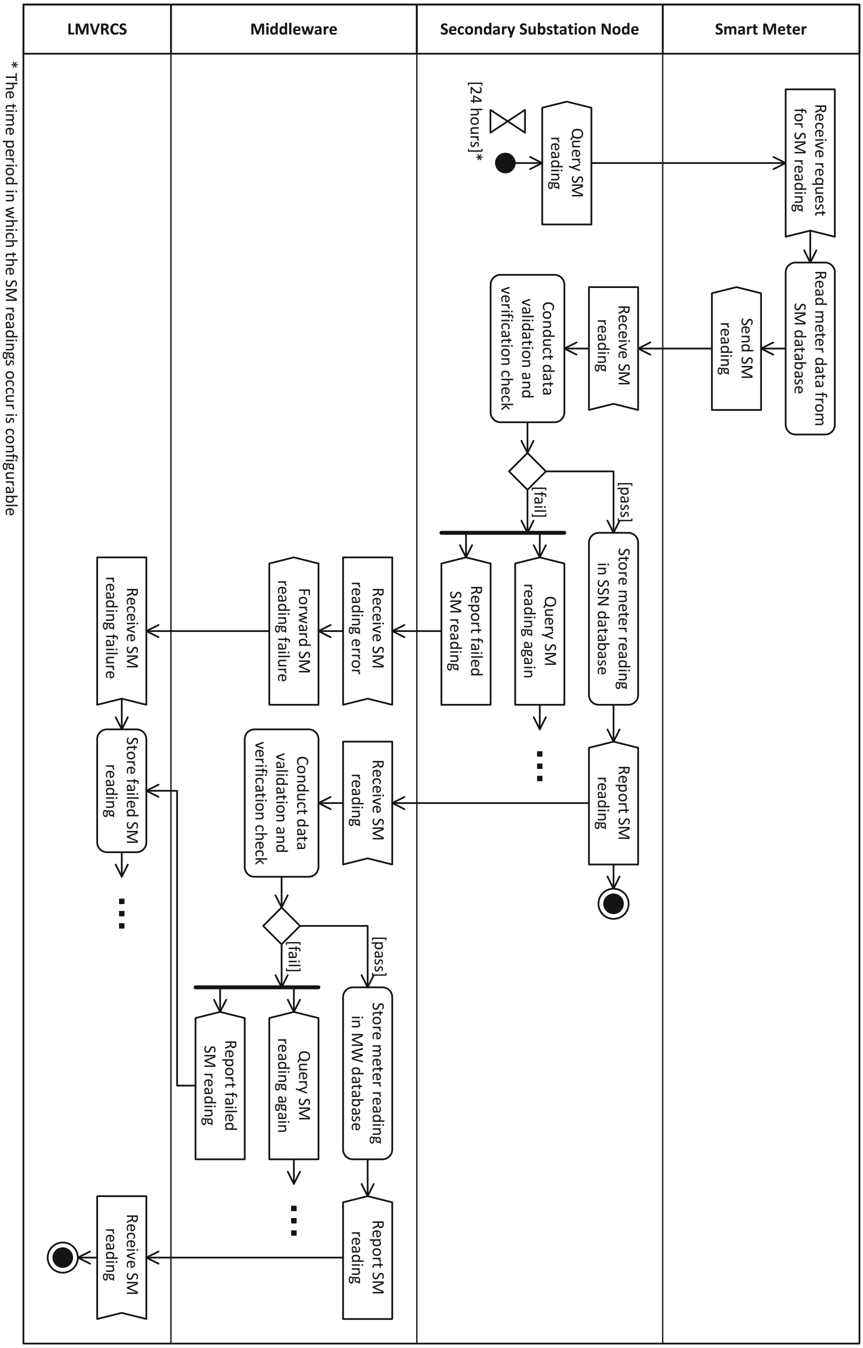
LMVRCS
Middleware
Secondary Substation Node
Smart Meter
[24 hours]*
Query SM reading
Receive request for SM reading
Read meter data from SM database
Send SM reading
Receive SM reading
Conduct data validation and verification check
[fail]
[pass]
Store meter reading in SSN database
Query SM reading again
Report failed SM reading
Receive SM reading error
Forward SM reading failure
Receive SM reading failure
Store failed SM reading
Report SM reading
Receive SM reading
Conduct data validation and verification check
[fail]
[pass]
Store meter reading in MW database
Query SM reading again
Report failed SM reading
Report SM reading
Receive SM reading
* The time period in which the SM readings occur is configurable

Fig. 3. Smart Meter reading process

Table 3. Scope exclusion table

Target element	Reason for scope exclusion
Secondary Substation (SS)	The SS is provided by the government and is protected by its security team
Secondary Substation Node (SSN)	The SSN is provided by the government and is protected by its security team
Middleware (MW)	The MW has a Common Criteria certification
...	...

Before concluding the description of the target, ISMS-CORAS requires the documentation and justification of any exclusions from the scope of the ISMS. This is documented in a scope exclusion table as exemplified in Table 3, which is an excerpt from the full table in the technical report.

Step 1.2: Specify Security Objectives and Assets. The client of the analysis (i.e. the commissioning party) is the energy supplier. Hence, the security risk analysis and the establishment of the ISMS is conducted for this party, and the security risks that we aim to identify are with respect to the security objectives and the assets of this party. However, the analysis is conducted from the viewpoint of the consumers in order to understand how security risks may arise due to the information processes involving the consumers and the smart homes.

The energy supplier is interested in analyzing privacy, integrity and confidentiality concerns of the consumers, and how these can be assured by establishing an ISMS. The following high-level security objectives are stated:

- The integrity, confidentiality, and availability of consumers' Home Agent configuration data shall be preserved
- The privacy of the consumers' energy consumption data shall be preserved
- The integrity, confidentiality, and availability of the consumers' Smart Appliances configuration data shall be ensured

The assets of the analysis are depicted in the CORAS asset diagram of Figure 4. The *Consumers' energy consumption data* shall be protected from attackers that may use this data for creating behavioral profiles. The value of the *Smart Appliances' configuration* to the consumer is essential, because without it the consumer loses control of the appliances in their home. For example, a stove could heat up during the night and cause a fire. The *Home Agents' configuration* states from/to which energy supplier the consumer buys/sells energy. An unauthorized change in the configuration could, for example, lead to the purchase of electricity at a too high price.

The arrows in the CORAS asset diagrams are so-called *harms* relations; a relation from one asset to another means that harm to the former may lead to harm to the latter. Hence harm to any of the three mentioned assets may cause harm to the *Consumers' security and privacy.*

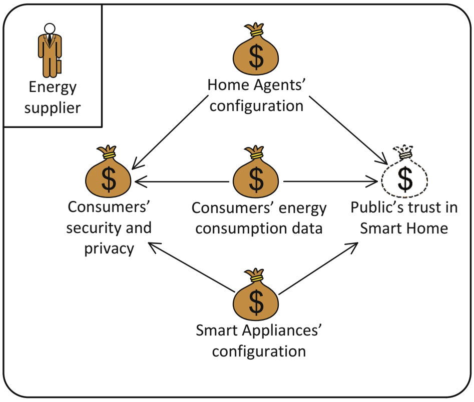
Energy supplier
Home Agents' configuration
Consumers' security and privacy
Consumers' energy consumption data
Public's trust in Smart Home
Smart Appliances' configuration

Fig. 4. Assets

In order to identify and assess risk, CORAS also includes so-called indirect assets. An indirect asset is an asset that, with respect to the target and scope of the analysis, is harmed only via harm to other assets. Hence, the risks are identified only with respect to the direct assets, but the risk estimation and evaluation also take into account the harm to the indirect ones. In our scenario the *Public's trust in Smart Home* is an indirect asset. We do not treat the indirect asset further in this chapter, and rather refer the reader to CORAS [28].

As a means to further focus the risk analysis, ISMS-CORAS requires the ranking of assets according to their relative importance. This is documented in an asset table as shown in Table 4, where 1 denotes the highest importance. The asset table also specifies the asset owner. Note that indirect assets are not included as risks with respect to these are identified via the direct assets, and the protection of these assets is the responsibility of the owners of the related direct assets.

Table 4. Asset table with ranking and owner

Asset	**Rank**	**Owner**
Consumers' energy consumption data	1	Mr. Jones
Smart Appliances' configuration	2	Mrs. Smith
Home Agents' configuration	3	Mr. Jones
Consumers' security and privacy	2	Mrs. Jackson

Existing controls for each asset are documented in the table format shown in Table 5, which is an excerpt from the corresponding table in the full technical report. These refer to controls implemented by the energy supplier, and are based on the controls specified by the ISO 27001 standard.

Table 5. Existing controls table

Asset	**Existing Control**
Consumers' energy consumption data	Secure communications between the SM and the SSN by encrypted data communication and encryption of all data on removable devices like SD-cards; data integrity by certificates and hash values
Home Agents' configuration	Access control: The prices and tariffs the SM can only be read by the customer; only the energy supplier is allowed to update prices and tariffs
...	...

Step 1.3: Conduct High-Level Security Risk Analysis. The high-level security analysis is conducted in order to get an initial understanding of the most important security risks, and to narrow down the scope of the analysis. The results are used to prioritize and structure the risk identification in Step 2. The attacker template and the attacker overview diagrams are ISMS-CORAS artifacts, whereas the high-level risk table is an extended version of the corresponding CORAS artifact. We have based the attacker template and attacker overview diagrams on the ideas behind misuse cases [37,44], which also rely on textual templates for describing misuse cases that attackers conduct, as well as corresponding UML use case diagrams [36]. The difference to our work is that ISMS-CORAS has a strong focus on security risk analysis, which is required for compliance with the ISO 27001 standard.

The ISMS-CORAS attacker template is shown in Table 6, and its instantiations give a structured way of describing attacker types, motivations, assumptions and resulting threat scenarios. The template consists of three parts, namely a *basic attacker description*, a *refined attacker description*, and *results*.

The basic attacker description starts with the definition of the attacker type, which is based on our previous work [6,9] where attackers are classified into the following categories. *Physical attacker*s threaten the physical elements of the system, e.g., hardware or buildings that host computers. *Network attacker*s threaten network connections within the target of analysis. *Software attacker*s threaten software components of the system, e.g., the smart meter. *Social engineering attacker*s threaten humans, e.g., the consumers. We reason about these types of attackers to determine whether they are relevant to our target of analysis, given its scope and assets. The reason for any exclusion of an attacker is that it cannot pose a threat to the target system and its assets. For example, if we analyze an autonomous system that has no humans in its scope, social engineering attackers do not need to be considered in the remaining analysis. All such reasons for exclusion of an attacker from the scope of the analysis have to be documented.

The usage of the template requires a statement about which assets are threatened by the attackers. The template has to be adjusted for each analysis according to the identified assets. We also state which of the security goals of confidentiality,

Table 6. Attacker template

Basic Attacker Description	
Attacker Type	□Physical Attacker □Network Attacker □Software Attacker □Social Engineering Attacker
Threatened Assets	□Asset 1 □Asset 2 □...
Threatened Security Goals	□Availability □Confidentiality □Integrity
	Reasoning
	– Explain why the selected security goals of an asset are threatened. – Reason also why the remaining security goals are excluded.
Entry Points	□Target Description Element 1 □Target Description Element 2 □...
	Reasoning
	– State why the selected elements are entry points for this attacker. – Reason why the remaining entry points are not relevant.
Attack Paths (possible vulnerabilities)	Describe all attack paths from the entry points to the assets.
Assumptions of the Target Description	□Target Description Element 1 □Target Description Element 2 □...
	Describe all assumptions about the target description.
Refined Attacker Description	
Required Attack Skills	State which kind of skills the attacker needs to succeed.
Attacker Motivation	□financial gain □self-interest □revenge □external pressure □curiosity
	Reasoning
	– Describe why the selected attacker motivations are relevant. – Explain also all exclusions of attacker motivations.
Required Resources	Describe the resources required for the attacker to conduct the attack.
Assumptions about the Attacker	Describe the assumptions about the motivation, skills, and resources of the attacker.
Insider / Outsider	Describe the difference if persons that are inside the scope and persons that are outside are the attacker.
Results	
Threats	Describe the high-level threats the attacker presents.
Reasons for Scope Exclusion	Describe the reasons for excluding the attacker or variants of the attacker from the scope of the threat analysis.

integrity, and availability that is/are threatened, and a reasoning of why any assets and security goals are selected or ruled out. The reasoning should be based on the attacker type.

The *entry points* and *attack paths* are based on Microsoft Threat Modeling [45]. This technique focuses on analyzing all interfaces of the target description elements to the outside world, and afterwards analyzing how an attacker can reach a particular asset from these entry points. A sequence of actions of an attacker leading him/her to the asset is a so-called *attack path*. An attack path without mitigating controls represents a vulnerability. Our attacker template has to be instantiated with the elements of the target description for each analysis.

A subsequent task is to reason about why an attacker can use an entry point or not, and to describe resulting attack paths. The last task for instantiating the first part of the attacker template is to specify assumptions about elements of the target description that reduce the number of entry points or attack paths.

The *refined attacker description* requires a description of the skills an attacker needs in order to succeed in harming the assets. The field *attacker motivation* is based on a study from the SANS Institute [3] that revealed four fundamental motivations of social engineering attackers: *Financial gain*, *self-interest*, *revenge*, and *external pressure*. We also added the motivation *curiosity*, which we identified in discussions with the industrial partners of the NESSoS project.

A subsequent task is to reason about why motivations are part of the scope of a particular attacker or why the motivations in regard to the attacker type and the threatened assets do not make sense. Existing threat classifications (such as the STRIDE classification [17]) can be used in combination with motivations to further facilitate the reasoning about attackers, in case threats do not come to mind immediately.

The *required resources* field describes the kind of resources, such as material and money, that the attacker requires to succeed in the attack. The instantiation of the template also involves the elicitation of *assumptions about the attacker*. The *insider/outsider* field shall invoke a reasoning of attackers that are part of the target description (insiders) and those that are not (outsiders). The *results* part of the template sums up the information collect about an attacker. This includes specifying the *threats* an attacker causes and also the *reasons for scope exclusions* of attackers.

In the technical report [10] we give examples of instantiated attacker templates for the smart home scenario for four kinds of attackers, namely a physical attacker, a network attacker, a software attacker and a social engineering attacker. Due to space constraints we omit these tables here, and show only the corresponding attacker overview diagram for the network attacker in Figure 5. Each such diagram always refers to one specific instantiation of the attacker template, and gives a brief and intuitive overview of the attacker, the attack entry points, the assets that may be harmed, as well as which of the security properties of confidentiality (C), integrity (I) and availability (A) that are affected. We have also identified a number of validation conditions to check the correctness and completeness of the attacker descriptions that are presented in the report.

The high-level security risk analysis takes into account the description of the target, the identified assets, and the instantiated attacker templates. The results serve as a means to further refine the scope and focus of the analysis, and to structure the risk identification of Step 2. The high-level risk table is exemplified with two entries in Table 7.

Note that there obviously are cases of attacks that involve the combination of attacker types. An attacker could, for example, target both network and software vulnerabilities at the same time. ISMS-CORAS allows for this by the possibility of considering more than one attacker type in the template. Such possible

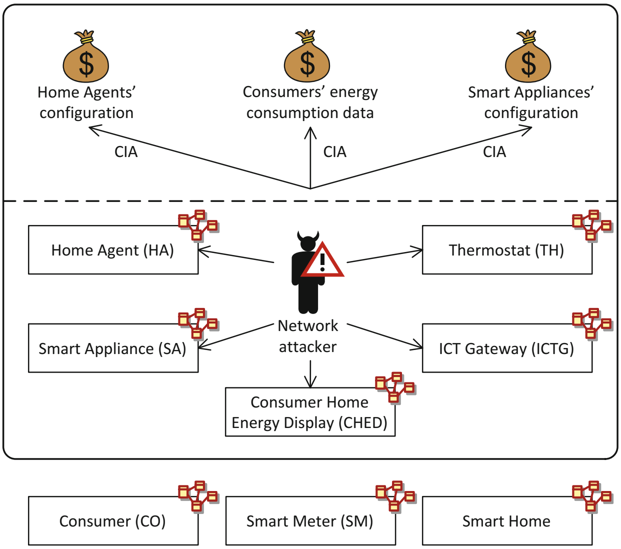

Fig. 5. Attacker overview diagram for network attacker

Table 7. High-level risk table

Who/what causes it?	**What is the incident? What is harmed?**	**What makes it possible?**	**What are the security objectives?**
Software attacker	Theft of energy consumption data	Insufficient malware detection	Consumers' privacy
Physical attacker	Housebreaking and destruction of Smart Meter	Insufficient physical protection	Availability of energy consumption data
...	...	...	...

combinations should also be identified and analyzed in more detail during the subsequent risk identification of Step 2.

Step 1.4: Define the Scales and the Risk Evaluation Criteria. This step is identical to CORAS, and includes the definition of scales for likelihoods and consequences. In the smart grid scenario we use qualitative scales of five values. In increasing order, the likelihoods are *rare*, *unlikely*, *possible*, *likely* and *certain*, whereas the consequences are *insignificant*, *minor*, *moderate*, *major* and *catastrophic*. We refer to the technical report for the more precise definition of the values since they are not important for the purpose of this chapter.

The risk evaluation criteria are shown in Figure 6, and distinguish between acceptable and unacceptable risks. The acceptable combinations of likelihoods and consequences are in light shading, whereas the unacceptable combinations are in dark shading.

Step 1.5: Identify Legal Aspects. The smart home scenario involves certain legal issues, and in our example both the German Energy Industry Act and the German Federal Data Protection Act (BDSG) apply. The latter refers to personal information, and according to [22,25,39], energy consumption data is personal information. We refer to the technical report for a detailed discussion of the implied legal issues, but mention only that the BDSG requires the informed consent of the person whose data is collected. In our scenario the metering data is collected once a day, and the shift to shorter intervals is an example of a possible violation.

In order to make the legal risk explicit in the analysis we introduce the asset of *Legal compliance*. We also define a consequence scale for this asset using the same terms as before, ranging from *insignificant* to *catastrophic*. See the technical report for further details.

4.2 Step 2: Identify Risks

The risk identification involves the identification and documentation of how threats and attackers may exploit vulnerabilities in order to initiate threat scenarios that lead to unwanted incidents. We give here a small and quite high-level example in order to illustrate the artefacts.

The risk identification refines the attacker descriptions and the high-level risk table by using CORAS threat diagrams. Figure 7 illustrates how ISMS-CORAS extends the CORAS threat diagram notation with the attacker motivation (depicted as a cloud) and the references from vulnerability to the target element that contains it. In our example a software attacker changes the Smart Meter configuration such that the frequency of readings is increased to every 15 minutes. A network attacker exploits a vulnerability in the ICT Gateway in order to steal energy consumption data.

In Figure 8 we show how Legal CORAS is used to take into account legal issues. As explained above, an increase in the frequency of Smart Meter readings may be

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Rare	░	░	░	░	▓
	Unlikely	░	░	░	▓	▓
	Possible	░	░	▓	▓	▓
	Likely	░	▓	▓	▓	▓
	Certain	▓	▓	▓	▓	▓

Fig. 6. Risk evaluation criteria; the light shading represents acceptable risk levels, while the dark shading represent unacceptable risk levels

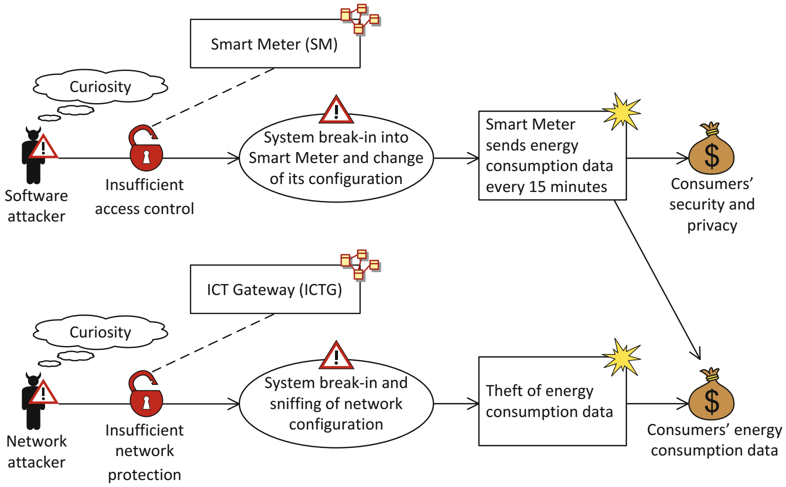
Smart Meter (SM)
Curiosity
Software attacker
Insufficient access control
System break-in into Smart Meter and change of its configuration
Smart Meter sends energy consumption data every 15 minutes
Consumers' security and privacy
ICT Gateway (ICTG)
Curiosity
Network attacker
Insufficient network protection
System break-in and sniffing of network configuration
Theft of energy consumption data
Consumers' energy consumption data

Fig. 7. Threat diagram

a violation of the BDSG. The diagram documents the legal norm that may apply when the incident *Smart Meter sends energy consumption data every 15 minutes* occurs. If the norm applies, this may lead to the incident of prosecution.

4.3 Step 3: Estimate Risks

This step is identical to CORAS, and involves the estimation of likelihoods and consequences of unwanted incidents. The results are documented by annotating the threat diagrams as illustrated in Figure 8. Legal uncertainties are also estimated and annotated on the identified legal norms. The latter is an estimate of the likelihood that the norm will actually apply under the identified circumstances. For the detailed explanation of the specific estimates we refer the reader to the full technical report.

4.4 Step 4: Evaluate Risks

The likelihood and consequence estimates are combined into risks using CORAS risk diagrams as exemplified in Figure 9. The risk levels (acceptable or unacceptable) are determined using the risk evaluation criteria as specified in the risk matrix of Figure 6. Note that because a risk is the combination of an unwanted incident and an asset, the incidents identified in Figure 8 represent four risks. In order to distinguish between them we give each risk a unique identifier (such as *SMS1* and *SMS2*). From Figure 9 and the filled in matrix in Figure 10 we see that there is one acceptable risk and three unacceptable.

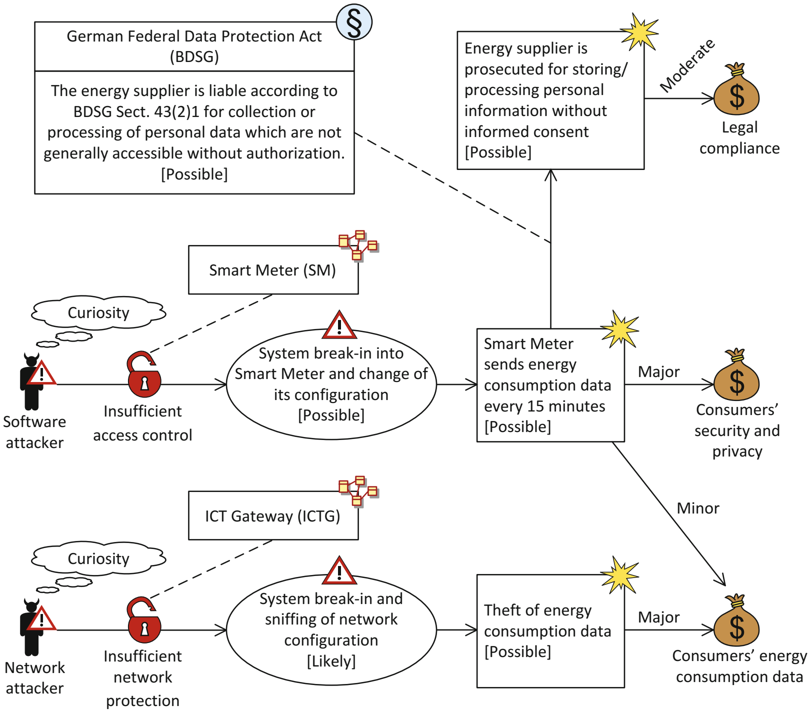
German Federal Data Protection Act (BDSG)
The energy supplier is liable according to BDSG Sect. 43(2)1 for collection or processing of personal data which are not generally accessible without authorization. [Possible]
Energy supplier is prosecuted for storing/ processing personal information without informed consent [Possible]
Moderate
Legal compliance
Smart Meter (SM)
Curiosity
Software attacker
Insufficient access control
System break-in into Smart Meter and change of its configuration [Possible]
Smart Meter sends energy consumption data every 15 minutes [Possible]
Major
Consumers' security and privacy
Minor
ICT Gateway (ICTG)
Curiosity
Network attacker
Insufficient network protection
System break-in and sniffing of network configuration [Likely]
Theft of energy consumption data [Possible]
Major
Consumers' energy consumption data

Fig. 8. Threat diagram with estimates

4.5 Step 5: Treat Risk

The unacceptable risks have to be evaluated for possible treatment. Appendix A of ISO 27001 describes a set of normative controls, and ISMS-CORAS requires these to be considered.

ISMS-CORAS provides support for the selection of controls by a mapping of controls to attacker types. Due to space constraints we do not present this mapping here, but rather refer to the full report. Each mapping refers to an ISO control (e.g. A.10.4 Protection against malicious and mobile code), an attacker type (e.g. software attacker), a control objective (e.g. integrity of software and information), and the relevant kind of target elements (e.g. critical software and services).

The identification and documentation of risk treatments are exemplified by the treatment diagram in Figure 11. The novelty of ISMS-CORAS is that the ISO 27001 controls have to be considered. The attacker motivation and related target elements are moreover specified, as for the extended threat diagram notation.

Each identified treatment points to the element of the threat diagram that it treats. The analyst may optionally annotate this relation with the treatment effect, which may be reduction of likelihood (*RL*) or reduction of consequence

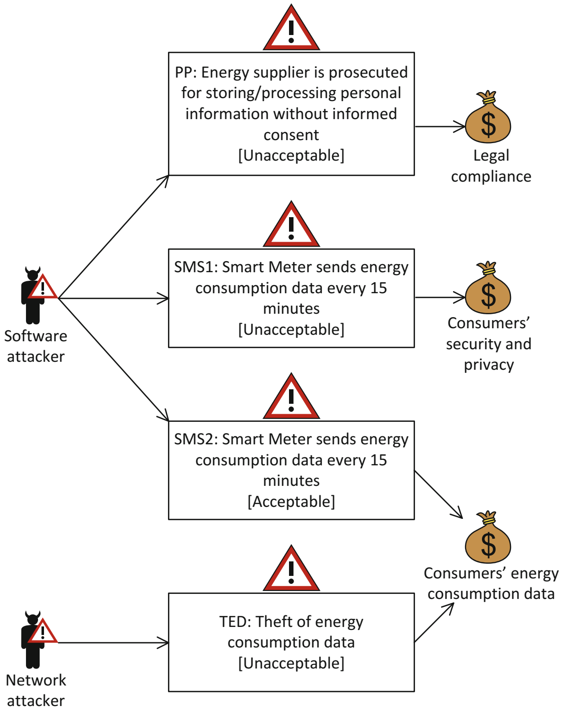
PP: Energy supplier is prosecuted for storing/processing personal information without informed consent
[Unacceptable]
Legal compliance
Software attacker
SMS1: Smart Meter sends energy consumption data every 15 minutes
[Unacceptable]
Consumers' security and privacy
SMS2: Smart Meter sends energy consumption data every 15 minutes
[Acceptable]
Consumers' energy consumption data
Network attacker
TED: Theft of energy consumption data
[Unacceptable]

Fig. 9. Risk diagram

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Rare					
	Unlikely					
	Possible		SMS2	PP	SMS1 TED	
	Likely					
	Certain					

Fig. 10. Risk evaluation

(*RC*). In Figure 11, controls for the protection of the ICT Gateway have been identified where, for example, improved network protection control may reduce the likelihood of a system break-in by a network attacker. Further treatments and their explanations are given in the report.

For the example of the use of the treatment overview diagrams, the treatment overview tables, the control exclusion table, the control effectiveness measure table and the ISMS procedure and control table, we refer the reader to the

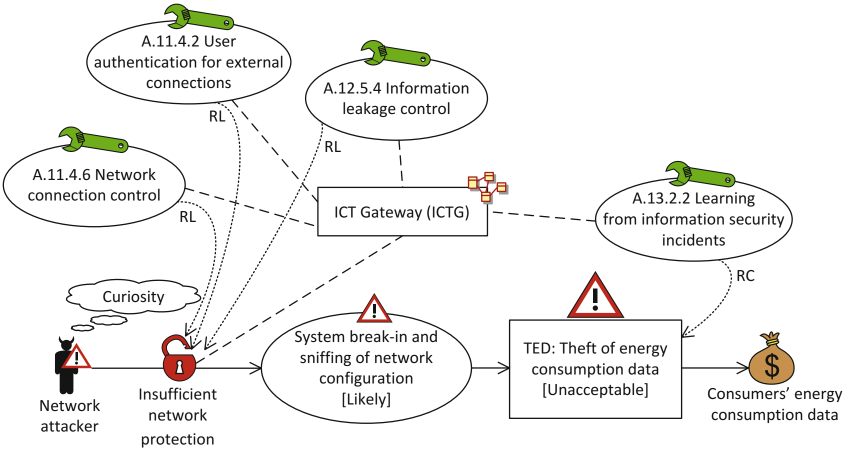
A.11.4.2 User authentication for external connections
A.12.5.4 Information leakage control
A.11.4.6 Network connection control
A.13.2.2 Learning from information security incidents
RL
RL
RL
RC
ICT Gateway (ICTG)
Curiosity
Network attacker
Insufficient network protection
System break-in and sniffing of network configuration [Likely]
TED: Theft of energy consumption data [Unacceptable]
Consumers' energy consumption data

Fig. 11. Treatment diagram

full technical report. These documentation artifacts documents the rationale for the treatment selection, including the related assets and security objectives, the responsible entities, as well as the necessary procedures and controls.

5 Related Work

To the best of our knowledge no specific methods for security requirements engineering or security risk analysis exist that support the establishment of an ISO 27001 compliant ISMS, and that satisfies the standard's documentation demands as is the goal of ISMS-CORAS.

Looking at established standards and methods for security risk analysis, several alternatives could be considered for facilitating the establishment of an ISMS, but none of them provide systematic support for ISO 27001 compliance. OCTAVE [2] is a suite of tools, techniques and methods for risk-based information security assessment and planning. Although the security risk analysis process is similar to ISMS-CORAS, the aim of OCTAVE is not to create and document an ISMS. The same is the case for CRAMM [42]. Both CRAMM and OCTAVE are compliant with the BS 7799 information security standard, which was adopted by ISO 27001. However, the focus is still on the security risk analysis, and less on systematically fulfilling the standard's requirements to ISMS establishment and documentation. The CRAMM repositories of assets, threats and countermeasures could, however, support the ISMS-CORAS process.

EBIOS [1] is a method for assessing and treating risks related to information systems security, and is consistent with the ISO 31000, ISO 27001 and ISO 27005 standards. While consistent with these standards, the method is designed for security risk identification and mitigation and provides therefore only partial support for establishing an ISO 27001 ISMS. The Microsoft Security

Risk Management Guide [33] is developed to support organizations in the overall security management and risk assessment. The fulfillment of ISO 27001 is beyond the scope, although there are many overlaps. The similar is the case for FRAAP [38], which is a method for analysis of information security related issues, focusing on protection of data confidentiality, integrity and availability.

Other existing works provide some guidance in interpreting the demands of the ISO 27001 standard. Calder [11] and Kersten et al. [23] provide advice for an ISO 27001 realization. In addition, Klipper [24] focuses on risk management according to ISO 27005. The author also includes an overview of the ISO 27000 series of standards. However, none of these works consider using structured methods to fully support the standard and its documentation requirements, as is the aim of ISMS-CORAS.

Other authors try to capture the most important relations presented in the standard by using models. Cheremushkin and Lyubimov [12] present a UML-based meta-model for several terms of the ISO 27000. These meta-models can be instantiated and, thus, support the refinement process [29]. However, the authors do not present a holistic method to information security.

Some existing approaches aim at improving the establishment of an ISMS via automation. Montesino et al. [34] investigate possible automation of controls that are listed in the ISO 27001 and ISO 27002. Their work can complement our own by providing some automation, but does not provide a complete method for establishing and documenting an ISMS.

For the Common Criteria (CC) standard [21] there exists a security requirements engineering approach that uses the standard as a baseline for a method. Mellado et al. [31] created the Security Requirements Engineering Process (SREP), which 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 [32]. The work differs from ours, because the authors do not support the ISO 27001 standard and also do not aim at security standard compliance or satisfying the Common Criteria documentation demands. In addition, Ardi and Shahmehri [5] extend the CC Security Target document with a section that considers knowledge of existing vulnerabilities. The authors aim at improving the CC and not at supporting its establishment.

6 Conclusion

In this chapter we have presented ISMS-CORAS, which is a structured method for establishing an information security management system (ISMS) that is compliant with the ISO 27001 standard. ISMS-CORAS is supported by techniques, modeling guidelines and documentation templates to ensure that all requirements to tasks and documentation are fulfilled. ISO 27001 defines the so-called Plan-Do-Check-Act (PDCA) model that specifies how to establish, implement, monitor and maintain an ISMS. ISMS-CORAS is developed to support the plan phase, and therefore focuses on the establishment and documentation of an ISMS.

Establishing an ISMS involves conducting a security risk analysis following a process similar to those defined by ISO 31000 and ISO 27005. Because CORAS is based on the former standard it already fulfills many of the ISO 27001 requirements to risk analysis and documentation. CORAS moreover comes with techniques, guidelines, modeling support and tool support that facilitate several parts of the ISO 27001 tasks. A further useful feature of CORAS in the ISMS context is the support for modeling and analyzing legal aspects.

ISMS-CORAS extends CORAS with the features, artefacts and techniques that are needed to provide complete support for establishing and documenting an ISMS. Some of the main novelties of ISMS-CORAS are the following. The method comes with detailed steps for asset identification, threat analysis, risk management and security reasoning; it is supported by attacker templates, classification of attacker types and attacker overview diagrams to facilitate and ensure completeness of attacker identification; it is supported by several kinds of diagrams for threat and risk modeling with attacker types, modeling of vulnerabilities and attacker entry points, as well as legal aspects; it provides a mapping between attacker types and ISO 27001 controls to facilitate treatment identification. These and other novelties in combination provide a systematic support for generating the required ISMS documentation in compliance with the standard.

As part of future work we plan to extend the approach to support all phases of the PDCA model, and not only the ISMS establishment of the plan phase. We will also conduct empirical studies to evaluate ISMS-CORAS and improve its usability. As part of the evaluation and validation, we moreover plan to compare ISMS-CORAS with alternative approaches to establish and document an ISO 27001 compliant ISMS. In particular, we will use publicly available tools such as verinice [47] and templates like the free ISO27k Toolkit [15] to create ISMS artifacts using the smart grid scenario presented in this chapter. The artifacts will serve as a basis for comparison and evaluation of ISMS-CORAS.

Acknowledgments. The research presented in this chapter was partially funded by the European Commission FP7 via the NESSoS (256980) network of excellence and the RASEN (316853) project.

References

1. Agence nationale de la sécurité des systèmes d'information: EBIOS 2010 – Expression of Needs and Identification of Security Objectives (2010) (in French)
2. Alberts, C.J., Dorofee, A.J.: OCTAVE Criteria. Tech. Rep. CMU/SEI-2001-TR-016, CERT (2001)
3. Allen, M.: Social engineering: A means to violate a computer system. SANS Institute Reading Room (2007)
4. Aloul, F., Al-Ali, A.R., Al-Dalky, R., Al-Mardini, M., El-Hajj, W.: Smart grid security: Threats, vulnerabilities and solutions. International Journal of Smart Grid and Clean Energy 1(1), 1–6 (2012)
5. Ardi, S., Shahmehri, N.: Introducing vulnerability awareness to Common Criteria's security targets. In: Fourth International Conference on Software Engineering Advances (ICSEA 2009), pp. 419–424. IEEE Computer Society (2009)

6. Beckers, K., Côté, I., Hatebur, D., Faßbender, S., Heisel, M.: Common Criteria CompliAnt Software Development (CC-CASD). In: Proceedings of the 28th Symposium on Applied Computing, pp. 937–943. ACM (2013)
7. 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)
8. Beckers, K., Faßbender, S., Küster, J.-C., Schmidt, H.: A pattern-based method for identifying and analyzing laws. In: Regnell, B., Damian, D. (eds.) REFSQ 2011. LNCS, vol. 7195, pp. 256–262. Springer, Heidelberg (2012)
9. Beckers, K., Hatebur, D., Heisel, M.: A problem-based threat analysis in compliance with Common Criteria. In: Proceedings of the International Conference on Availability, Reliability and Security (ARES 2013), pp. 111–120 (2013)
10. Beckers, K., Heisel, M., Solhaug, B., Stølen, K.: ISMS-CORAS – A structured method for establishing an ISO 27001 compliant information security management system. Tech. Rep. A25626, SINTEF ICT (2013)
11. Calder, A.: Implementing Information Security based on ISO 27001/ISO 27002: A Management Guide. Haren Van Publishing (2009)
12. Cheremushkin, D.V., Lyubimov, A.V.: An application of integral engineering technique to information security standards analysis and refinement. In: Proceedings of the 3rd International Conference on Security of Information and Networks (SIN 2010), pp. 12–18. ACM (2010)
13. Evaluation of general requirements according state of the art. OpenNode project deliverable D1.2 (2010)
14. Faßbender, S., Heisel, M.: From problems to laws in requirements engineering – Using model-transformation. In: International Conference on Software Paradigm Trends (ICSOFT 2013), pp. 447–458. SciTePress (2013)
15. FREE ISO27k Toolkit,
    http://www.iso27001security.com/html/iso27k_toolkit.html
    (accessed January 21, 2014)
16. Functional use cases. OpenNode project deliverable D1.3 (2010)
17. Howard, M., LeBlanc, D.: Writing Secure Code, 2nd edn. Microsoft Press (2003)
18. International Organization for Standardization: ISO 31000 – Risk management – Principles and guidelines (2009)
19. International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements (2005)
20. International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 27005 – Information technology – Security techniques - Information security risk management (2008)
21. International Organization for Standardization / International Electrotechnical Commission: ISO/IEC 15408 – Common Criteria for Information Technology Security Evaluation (2009)
22. Karg, M.: Datenschutzrechtliche Bewertung des Einsatzes von "intelligenten" Messeinrichtungen für die Messung von gelieferter Energie (Smart Meter). Tech. rep., Unabhängiges Landeszentrum für Datenschutz (ULD) (2009) (in German)
23. Kersten, H., Reuter, J., Schröder, K.W.: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Vieweg+Teubner (2011) (in German)

24. Klipper, S.: Information Security Risk Management mit ISO/IEC 27005: Risikomanagement mit ISO/IEC 27001, 27005 und 31010. Vieweg+Teubner (2010) (in German)
25. Knyrim, R., Trieb, G.: Smart metering under EU data protection law. International Data Privacy Law 1(2), 121–128 (2011)
26. Kreutzmann, H., Vollmer, S.: Protection profile for the gateway of a smart metering system (Smart meter gateway PP). Tech. Rep. BSI-CC-PP-0073, Federal Office for Information Security, version 1.2, Final Release (2013)
27. Lin, H., Fang, Y.: Privacy-aware profiling and statistical data extraction for smart sustainable energy systems. IEEE Transactions on Smart Grid 4(1), 332–340 (2013)
28. Lund, M.S., Solhaug, B., Stølen, K.: Model-Driven Risk Analysis – The CORAS Approach. Springer (2011)
29. Lyubimov, A., Cheremushkin, D., Andreeva, N., Shustikov, S.: Information security integral engineering technique and its application in ISMS design. In: Sixth International Conference on Availability, Reliability and Security (ARES 2011), pp. 585–590. IEEE Computer Society (2011)
30. Mahler, T.: Legal Risk Management – Developing and Evaluating Elements of a Method for Proactive Legal Analyses, With a Particular Focus on Contracts. Ph.D. thesis, University of Oslo (2010)
31. Mellado, D., Fernandez-Medina, E., Piattini, M.: A comparison of the Common Criteria with proposals of information systems security requirements. In: The First International Conference on Availability, Reliability and Security (ARES 2006), pp. 654–661. IEEE Computer Society (2006)
32. 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)
33. Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence: The Security Risk Management Guide (2006)
34. Montesino, R., Fenz, S.: Information security automation: How far can we go? In: Sixth International Conference on Availability, Reliability and Security (ARES 2011), pp. 280–285. IEEE Computer Society (2011)
35. Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS), http://www.nessos-project.eu/ (accessed December 19, 2013)
36. Object Management Group: OMG Unified Modeling Language (OMG UML), Superstructure. Version 2.3, OMG Document: formal/2010-05-03 (2010)
37. Opdahl, A.L., Sindre, G.: Experimental comparison of attack trees and misuse cases for security threat identification. Inf. Softw. Technol. 51, 916–932 (2009)
38. Peltier, T.R.: Information Security Risk Analysis, 3rd edn. Auerbach Publications (2010)
39. Raabe, O., Lorenz, M., Pallas, F., Weis, E.: Datenschutz im Smart Grid und in der Elektromobilität. Tech. rep., Karlsruher Institut für Technologie, KIT (2011) (in German)
40. Report on the identification and specification of functional, technical, economical and general requirements of advanced multi-metering infrastructure, including security requirements. OPEN meter project deliverable D1.1 (2009)
41. Rodden, T.A., Fischer, J.E., Pantidi, N., Bachour, K., Moran, S.: At home with agents: Exploring attitudes towards future smart energy infrastructures. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2013, pp. 1173–1182. ACM (2013)

42. Siemens: CRAMM – The total information security toolkit, `http://www.cramm.com/` (accessed: January 15, 2013)
43. Siemens: No longer a one-way street, `http://www.siemens.com/innovation/apps/pof_microsite/_pof-spring-2011/_html_en/smart-grids.html` (accessed December 19, 2013)
44. Sindre, G., Opdahl, A.L.: Templates for misuse case description. In: Procedings of the 7th International Workshop on Requirements Engineering, Foundation for Software Quality (REFSQ 2001), pp. 4–5 (2001)
45. Swiderski, F., Snyder, W.: Threat Modeling. Microsoft Press (2004)
46. Tran, L.M.S., Solhaug, B., Stølen, K.: An approach to select cost-effective risk countermeasures. In: Wang, L., Shafiq, B. (eds.) DBSec 2013. LNCS, vol. 7964, pp. 266–273. Springer, Heidelberg (2013)
47. verinice, `http://www.verinice.org` (accessed January 21, 2014)