SINTEF

SINTEF A25626- Unrestricted

Report

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

Authors
Kristian Beckers
Maritta Heisel
Bjørnar Solhaug
Ketil Stølen

SINTEF ICT
Networked Systems and Services
2013-12-10

SINTEF IKT
SINTEF ICT

Address:
Postboks 124 Blindern
NO-0314 Oslo
NORWAY

Telephone:+47
Telefax:+47 22067350

Enterprise /VAT No:

SINTEF

SINTEF IKT
SINTEF ICT
Address:
Postboks 124 Blindern
NO-0314 Oslo
NORWAY
Telephone:+47
Telefax:+47 22067350

Enterprise /VAT No:

KEYWORDS:
Security standards,
requirements
engineering,
risk management,
ISO 27000,
ISO 27001,
compliance,
security,
CORAS

Report

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

VERSION
1.0

DATE
2013-12-10

AUTHOR(S)
Kristian Beckers
Maritta Heisel
Bjørnar Solhaug
Ketil Stølen

CLIENT(S)
European Commission

CLIENT'S REF.
FP7 NoE NESSoS (256980)

PROJECT NO.
102002252

NUMBER OF PAGES/APPENDICES:
69 incl. appendix

ABSTRACT
Realizing security and risk management standards may be challenging, partly because the descriptions of what to realize are often generic and have to be refined by security experts. Removing this ambiguity is time intensive for security experts, because the experts have to interpret all the required tasks in the standard on their own. In our previous work we showed how to use security requirements engineering methods for the development and documentation of the ISO 27001 security standard. In this paper we (i) create an extension of the CORAS methodology for risk management that supports the ISO 27001 standard, (ii) validate the method via comparing its resulting artifacts to the artifacts of an industrial ISO 27001 application, and (iii) discuss the advantages of our method compared to the industrial state-of-the-art. We apply our method to a smart grid scenario provided by the industrial partners of the NESSoS project.

PREPARED BY
Bjørnar Solhaug

SIGNATURE


CHECKED BY
Atle Refsdal

SIGNATURE


APPROVED BY
Bjørn Skjellaug

SIGNATURE


REPORT NO.	ISBN	CLASSIFICATION	CLASSIFICATION THIS PAGE
SINTEF A25626	978-82-14-05338-8	Unrestricted	Unrestricted

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

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

[1] paluno, University of Duisburg-Essen, Germany
{firstname.lastname}@paluno.uni-due.de
[2] SINTEF ICT, Norway
{firstname.lastname}@sintef.no
[3] Dep. of Informatics, University of Oslo, Norway

Abstract. Realizing security and risk management standards may be challenging, partly because the descriptions of what to realize are often generic and have to be refined by security experts. Removing this ambiguity is time intensive for security experts, because the experts have to interpret all the required tasks in the standard on their own. In our previous work we showed how to use security requirements engineering methods for the development and documentation of the ISO 27001 security standard. In this paper we (i) create an extension of the CORAS methodology for risk management that supports the ISO 27001 standard, (ii) validate the method by comparing its resulting artifacts to the artifacts of an industrial ISO 27001 application, and (iii) discuss the advantages of our method compared to the industrial state-of-the-art. We apply our method to a smart grid scenario provided by the industrial partners of the NESSoS project.

Keywords: security standards, requirements engineering, risk management, ISO27000, ISO27001, compliance, security, CORAS

1 Introduction

Fulfilling organizations' security needs is a challenging task, but various security standards, e.g., ISO 27001 [1], offer ways to attain this goal. The mentioned standard prescribes a process for establishing and maintaining a so-called *Information Security Management System* (ISMS), which tailors security to the needs of any kind of organization. However, several ambiguities in the standard may cause challenges during the establishment of an ISMS. For example, the required input for the *scope and boundaries* description includes "characteristics of the business, the organization, its location, assets, and technology"[1, p. 4]. This security standard is ambiguous on purpose, because it should serve a multitude of different domains and stakeholders. The ambiguity

* This research was partially supported by the EU FP7 Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS, ICT-2009.1.4 Trustworthy ICT, Grant No. 256980).

is nevertheless a problem for security experts who have to choose a method for security analysis that is compliant with the standard. These experts moreover need to decide the abstraction level for the required documentation without any support from the standard. In our example, security experts have to describe the business, organization, 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, assets and other elements within the desired scope. Moreover, the standard does not provide a method for assembling the necessary information, or a pattern or template for structuring this information. The importance of these steps becomes apparent when one realizes that essential further steps of the ISO 27001 depend upon them, including the identification of *threats*, *vulnerabilities* and *controls*.

We propose an extension of the CORAS method [2] 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 [3], and our results showed that the ISO 27001 standard has a significant focus on risk analysis. The ISO 27001 Sect. 4.2.1 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 [4] standard, which is also the basis for the risk management process of ISO 27005 [5]. 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* [2]. CORAS also comes with tool support for all phases of the process, and the tool ensures the syntactically correct use of the CORAS notation.[4] CORAS moreover facilitates the reporting of the results by a formal mapping from 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 concerns, 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 [2].

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 that the industrial partners of the NESSoS project provided.

The outline of the report is as follows. In Section 2 we present the most important background to ISMS-CORAS, which includes CORAS, Legal CORAS and the ISO 27001 standard. In Section 3 we present the ISMS-CORAS method by describing its steps, how it extends CORAS, how it supports the establishment of an ISO 27001 compliant standard, and how it produces the artefacts necessary for generating the required documentation. In Section 4 we demonstrate the application of ISMS-CORAS

[4] The CORAS Tool homepage: `http://coras.sourceforge.net/coras_tool.html`

on a smart grid scenario. We discuss related work in Section 5 before we conclude in Section 6. We have also included an appendix in which we make a comparison of the terms and processes defined by ISO 31000, ISO 27001 and CORAS. This is to identify the similarities and differences, and to clarify how we use the relevant terms in ISMS-CORAS.

2 Background

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

2.1 CORAS

CORAS is a method for risk analysis that follows the process defined by the ISO 31000 risk management standard. The overall process includes the following consecutive steps.

The first step is *establishing the context*, which is divided into four steps in CORAS. The objective of the context establishment is to specify the target of analysis, define the focus, scope and assumptions, specify the assets, and define the risk evaluation criteria. Based on an initial target description from the customer, the risk analysts develop a *(semi-)formal target description* in order to precisely document the target of analysis at an adequate level of abstraction. The identified assets, with respect to which the subsequent risk assessment is conducted, are documented using a CORAS *asset diagram*.

A *high-level risk table* describes threats to these assets, as well as the potential cause of the threats. The step also includes defining the *likelihood and consequence scales* that will be used for estimating and evaluating the risks, and the *risk matrices* that are used for defining the risk evaluation criteria. All of these artifacts are presented to the customer who needs to approve them in written form in order to complete the context establishment part.

The risk assessment incudes *risk identification*, *risk estimation* and *risk evaluation*. The risk identification is to identify threats, vulnerabilities, threat scenarios and unwanted incidents. Conducting this task and documenting the results are supported by CORAS *threat diagram*s. 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 determine which risks that 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, etc.

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 [2] is an extension of CORAS specifically for considering legal aspects and legal risk. The initial target description in Legal CORAS contains a statement about whether and to what extent legal aspects should be considered in the risk analysis. The method elicits relevant legal aspects based upon the final target description.

The source of legal risks is legal norms, which are norms that stem from a legal source such as laws, regulations, contracts and legally binding agreements. When assessing legal risks, 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* [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.

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 PDCA. 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 (see ISO 27001 Sect. 4.3.1 and Sect. 5), which we introduce in the following. The names of the ten documents are printed in italics[5].

(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*[6] that can provide evidence of compliance to the requirements of the ISMS, and (9) the *Statement of Applicability* "describing the control objectives and controls that are relevant and applicable to the organization's ISMS." [1, p. 3]. In addition, the ISO 27001 standard demands the

[5] The ISO 27001 demands documents with a certain content. We choose to give these documents names in order to avoid verbal descriptions each time we refer to a certain content.

[6] The ISO 27001 Sect. 4.3.2 and 4.3.3 concern control of documents and records. For simplicity's sake, we are not showing how to address these demands in this paper.

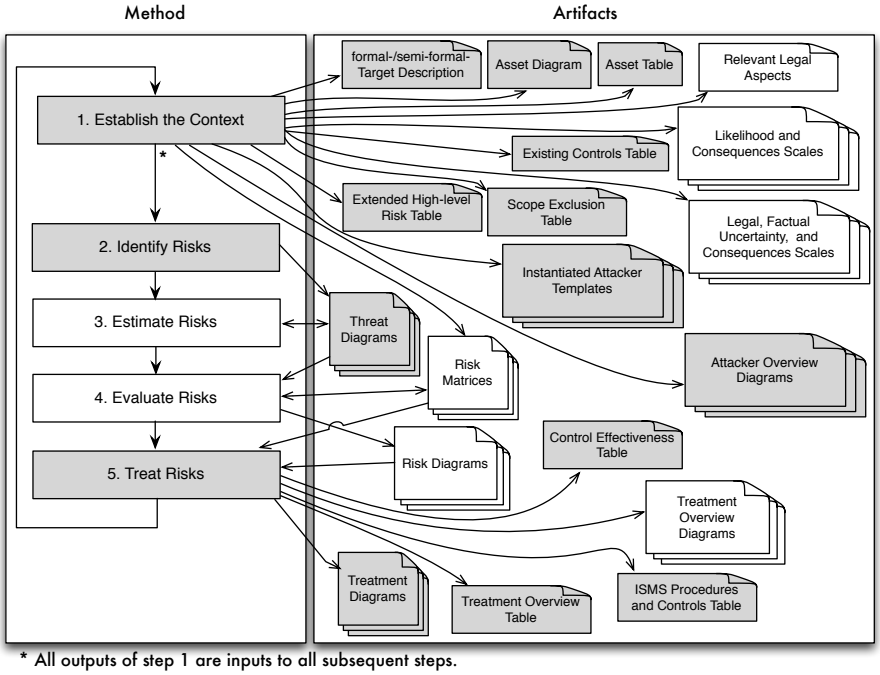

Fig. 1. The ISMS-CORAS Method

documentation of (10) *Management Decisions* that provide support for establishing and maintaining an ISMS.

3 The ISMS-CORAS Method

The method presented in this section extends CORAS in order to support security management compliant with ISO 27001. Our contribution, namely *ISMS-CORAS*, follows the steps depicted to the left in Fig. 1. The figure also shows the resulting artifacts from applying our method. While keeping the names of the method steps, we focus in our description on the difference to CORAS, and we explain how our changes to CORAS are related to ISO 27001 and its documentation requirements as described above. The CORAS steps that we modified and extended in developing ISMS-CORAS are marked in grey in the figure. The same is the case for the novel or modified arifacts depicted to the right.

Note, importantly, 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.” [1, p. 8]. Hence, we can use CORAS artifacts in the creation of our ISMS documentation.

Step 1: Establish the Context - The purpose of this step remains unchanged, which is to develop the target description and set the scope and focus of the security risk analysis. Before arriving at a (semi-)formal target description it is allowed to create informal descriptions as a basis for discussion between the security analyst and the customer. Step 1 fulfills the demands of ISO 27001 Sect. 4.2.1a, which concerns the addition of characteristics of the business, and information about technology relevant to the target description.

A specific subtask concerns the documentation of scope exclusions in a *scope exclusion table*. The table refers to elements in the target description and state a reason for excluding this particular element from the scope of the analysis. It is moreover mandatory to consider legal aspects in ISMS-CORAS, because the ISMS policy (see Sect. 2.3) defined in ISO 27001 Sect. 4.2.1b requires this action. In Legal CORAS this is a choice of the customer. The identification of relevant legal aspects can be achieved, e.g., via using our law patterns method [6, 7] or by involving domain experts and lawyers.

ISMS-CORAS requires an explicit description of the location of each element in the target description, due to demands of ISO 27001 Sect. 4.2.1a. Moreover, the location information is also essential for the consideration of legal aspects. For example, according to the German Federal Data Protection Act (BDSG) Sect. 4b, it is not allowed to store personal information outside of the European Union.

The step describes further how to use the target description to identify assets, which are documented using asset diagrams following the CORAS process. The assets are anything the customer values within the scope of the analysis. ISO 27001 uses a similar definition for assets [1, p. 2], but the standard states also that the ISMS is built in particular to protect *information assets* [1, p. 1]. CORAS uses the term asset in a broader sense and considers also, e.g., physical assets such as computers. This view is in accordance with ISO 31000. Hence, ISMS-CORAS considers assets also in a broader sense, but some tasks concern only information assets. We make this clear distinction because all of the subsequent ISMS-CORAS tasks are driven by the assets. The asset identification is a means to specify the main focus of the analysis, and the risk assessment is with respect to this focus area only. Another task is to rate all assets according to their importance in order to prioritize the risk assessment according to ISO 27001 Sect. 4.2.1d. The rating and priority are documented in *asset table*s. ISMS-CORAS requires also the definition of asset owners in these tables. *Asset owner* is an "individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. Note that the term 'owner' does not mean that the person actually has any property rights to the asset." [1, p. 4]

Moreover, the first step of ISMS-CORAS involves the documentation of existing security controls. These shall be discussed when refining the target description and documented in an *existing controls table*, which lists the controls and the assets these controls protect.

ISMS-CORAS aims to identify relevant vulnerabilities of the systems in the ISMS scope, and also threat scenarios in order to describe, for example, how an attacker may exploit a vulnerability. This step relies upon further refinement of the elements in the scope of the ISMS. ISMS-CORAS stresses in this step the identification of vulnerabilities, due to ISO 27001 Sect. 4.2.1d demands. This section of the standard also states

that the possible impact an exploitation of each vulnerability has on the information asset must be estimated. The documentation of this impact shall consider confidentiality, integrity and availability. We use attacker templates to reason about attacker types and attacker motivations in relation to assets and the target description (see Sect. 4.1). The instantiation of these templates results in documenting attackers that are out of scope and assumptions that lead to scope exclusions. Their documentation is vital in order for other security experts to follow the reasoning of the threat model, e.g., in an audit of the ISMS. The remaining attackers, their entry points in the target description, and the threatened assets are documented in attacker overview diagrams. These specify also the elements of the target descriptions and assets that are out of reach of a particular attacker, and therefore can be excluded from further analysis. Attacker templates and attacker overview diagrams are contributions of ISMS-CORAS.

Step 1 also involves the creation of a *high-level risk table* that defines who or what may cause incidents, how the threat harms the assets, and the vulnerabilities that the threat potentially exploits. ISMS-CORAS fulfills the ISO 27001 Sect. 4.2.1d demands for a specific consideration of availability, confidentiality and integrity for information assets, as well. These are documented in an *extended high-level risk table* as the high-level security objectives that should be achieved. The risks and necessary mitigations should be identified with respect to these objectives. For example, a security objective may be the protection of the confidentiality of health records.

Several subtasks concerning the initial risk assessment have to be conducted according to ISO 27001 Sect.4.2.1c. The first is the definition of the risk assessment methodology, which is in our case the ISMS-CORAS method. The scales for likelihoods and consequences have to be determined, and the risk evaluation criteria must be formulated. For this purpose, we create *risk matrices*, which contain ratings of all combinations of consequences and likelihoods to acceptable and unacceptable risks. Risks caused by legal issues are also considered in the specification of scales for legal uncertainty. All of these risk assessment aspects have to be aligned with existing risk management efforts that already exist for the scope of the analysis, as stated in ISO 27001 Sect. 4.2.1b. CORAS concludes this step with written approval of the customer of the target description and target models. We extend this subtask with written management commitment and resource commitment for the ISMS according to ISO 27001 Sects. 5.1 and 5.2. This includes the consideration of, e.g., external audits of the ISMS.

Contribution to ISMS documents: Scope of the ISMS, ISMS Policy Statements, Risk Assessment Report, Management Decisions, Procedures and Controls in Support of the ISMS

Step 2: Identify Risk - In this step CORAS proposes to use structured brainstorming as a risk identification technique. This task demands the consideration of the elicited threats in the previous step and all other available information, as well. This leads to a refinement of the attacker descriptions and also to the identification of further relevant legal aspects. The identified threats, vulnerabilities, threat scenarios, unwanted incidents, and legal aspects are documented in CORAS threat diagrams.

Contribution to ISMS documents: Risk Assessment Report

Step 3: Estimate Risk - This step determines the risk levels of the risks caused by the unwanted incidents in the previous step. CORAS uses brainstorming techniques and other available sources of information, e.g. logs of system attacks, to estimate likelihoods and consequences of these unwanted incidents. The risk estimation is moreover facilitated by the CORAS calculus for reasoning about likelihoods in CORAS threat diagrams. ISMS-CORAS focuses on the likelihood estimation on misuses or exploits of the identified vulnerabilities. A task during the brainstorming is to derive attacker types with a certain skill set, similar to the descriptions proposed in the Common Criteria [8]. The results of this step are documented in threat diagrams. A further task in ISMS-CORAS is to estimate legal and factual uncertainty of the identified legal norms according to the description of Legal CORAS.

Contribution to ISMS documents: Risk Assessment Report

Step 4: Evaluate Risk - The fourth step aims to decide if risks are acceptable or require treatment. ISMS-CORAS is identical to CORAS at this step, and uses the risk evaluation criteria and the results of the risk estimation for this decision.

Contribution to ISMS documents: Risk Assessment Report

Step 5: Treat Risk - The fifth step concerns the identification and analysis of treatments for unacceptable risks. This treatment should reduce risk levels by reducing the likelihood and/or consequence of unwanted incidents. ISMS-CORAS restricts the identification of risk treatments to the normative controls defined in Appendix A of the ISO 27001 standard. The treatments have to consider existing controls, and the asset owner is responsible for the controls protecting the asset. This information has to be included in the treatment diagrams and treatment overview diagrams. The residual risk has to be documented and the management has to approve it.

The treatment plans should consider cost-benefit reasoning, e.g., by using the CORAS extension proposed in [9]. Step 5 requires further a reasoning of why a particular Appendix A control is considered or left out. For this purpose we propose to use treatment overview tables that refer to an asset, its security objective, and relevant treatment or treatment overview diagrams, and a reasoning of why the treatment is sufficient.

We also have to document how the effectiveness of each control can be measured in a *control effectiveness table* that defines measures to assess the effectiveness of each control. The procedures and controls that are part of the ISMS have to be documented. A further subtask is to document each procedure that is part of a selected control. After the selection of all controls the ISO 27001 Sect. 4.2.1g demands a conflict analysis between the selected controls and legal aspects. For this reason, we have to apply Legal CORAS considering all selected controls. The management has to provide an authorization to implement and operate the resulting ISMS, and this approval requires documentation.

Contribution to ISMS documents: Risk Treatment Plan, Statement of Applicability, Procedures and Controls in Support of the ISMS, Procedures to the effective planning, operation and control of the ISMS, Management Decisions

Table 1. ISMS-CORAS support for the ISO 27001 Documentation Demands

Nr.	ISO 27001 Documents	ISMS-CORAS Artifacts	Step
1.	Scope of the ISMS	(Semi-)Formal target description, Scope exclusion table	1
2.	ISMS Policy Statements	Extended high-level risk tables	1
3.	Procedures and Controls in Support of the ISMS	ISMS procedure table	1,5
4.	Risk Assessment Methodology	Description of the ISMS-CORAS method	1-5
5.	Risk Assessment Report	Asset diagrams, Asset tables, Likelihood scales, Consequence scales, Risk matrices, Threat diagrams, Risk diagrams, Likelihood and consequence estimates	1-4
6.	Risk Treatment Plan	Treatment diagrams, Treatment overview diagrams with responsibilities	5
7.	Procedures to the effective planning, operation and control of the ISMS	Treatment diagrams, Treatment overview table, Control effectiveness table, Written documentation	5
8.	ISMS Records	N/A	
9.	Statement of Applicability	Treatment diagrams, treatment overview table	5
10.	Management Decisions	Written documentation	1,5

We show how ISMS-CORAS fulfills the ISO 27001 documentation demands (see ISO 27001 Sect. 4.3.1 and Sect. 5) in Tab. 1. The first column states the number we assigned to each document, the second the name of the ISO 27001 document as introduced in Sect. 2.3, the third the ISMS-CORAS artifacts from which the ISO 27001 document is created, and the last column states the steps of ISMS-CORAS that contribute to the creation of the artifacts. Recall from Section 2.3 that the use of ISMS Records is outside the scope of ISMS-CORAS.

4 Application of our Method

In this section we demonstrate the use of ISMS-CORAS by applying the method to a smart grid scenario. 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 technologies (ICT). A novelty compared to existing energy networks is the two-way communication between consumers and electric power companies. The benefits of the smart grid are envisioned to be a more economic, sustainable and reliable supply of energy. However, significant security concerns have to be addressed for this scenario, due to the possible dangers of missing availability of energy for customers, as well as threats to the integrity and confidentiality of customer's data. These concerns are of particular relevance, because energy grids have a significantly longer lifespan than telecommunication networks [10]. In addition, privacy concerns have risen, such as the possibility of creating behavioral profiles of customers if their energy consumption is transmitted over the smart grid in small time intervals [11].

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 [2].

4.1 Step 1: Establish the Context

The smart home scenario is provided by the industrial partners of the NESSoS[7] project. The scenario concerns a house that is divided into two living units of separate electricity consumers. In the application of ISMS-CORAS we have used the UML [12] to model the target of analysis and specify the desired scope and focus. More specifically, we used a class diagram for modeling the architecture and activity diagrams to model the relevant behavior.

In the class diagram of Fig. 2, the associations represent communication connections. All elements within the scope of the analysis are the elements of the target description that are inside the smart home. For simplicity's sake we do not include the smart home in the UML model, and we do not consider the transport and production of energy. The focus of the analysis is on the communication of information in the scenario. This is partly due to the fact that the ISO 27001 ISMS is only concerned with information assets (see Sect. 3). The indicated location of the entities are based on real smart grid experiments conducted by the NESSoS partners in Germany[8].

The analysis is conducted on the behalf of the energy supplier, and the goal is to protect the assets of the supplier. However, the viewpoint on the target of analysis is of the customers, meaning that the focus is on customer data and the customers' use of the smart home.

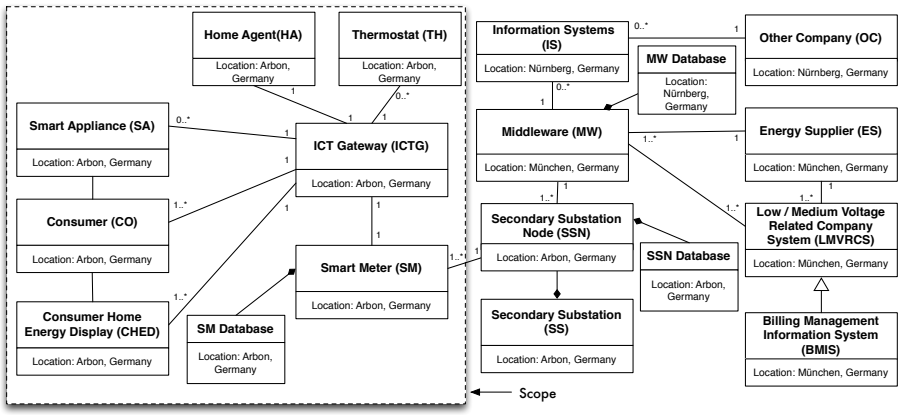

Fig. 2. The semi-formal target description of the NESSoS Smart Home scenario

The *ICT Gateway (ICTG)* is the connection between the smart home and the information systems of the *Energy Supplier (ES)*. Every party in the smart home consists of

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

[8] http://www.siemens.com/innovation/apps/pof_microsite/_pof-spring-2011/_html_de/smart-grids.html

Consumers (CO), 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 in the evening. 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 of SAs. The temperature information is used for safety purposes, e.g., to prevent 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 ES [13]. Every consumer has its own *Smart Meter (SM)*, which is placed in the cellar of the smart home.

The two consumers in this scenario share the cellar. The SM measures the energy consumption and sends the consumption information in hourly 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 produced energy and sends the information to the ES.

The SM transfers the energy consumption/production data to the *Secondary Substation Node (SSN)*, which is part of the *Secondary Substation (SS)*. The SS transforms voltage from high to low and transmits it to the energy consumers. The energy comes from electrical generation facilities. The SS also receives energy from consumers and distributes it to other consumers. SSNs are intelligent computerized units that are specific components of smart grids. These units have the ability to communicate to each other and guide the energy flow within smart grids. The *SSN Database* is an internal storage device inside the SSN. SSNs also communicate with the *Middleware (MW)* of the ES, which in turn communicate with the *Low/Medium Voltage Related Company Systems (LMVRCS)* of the ES. The MW also contains an internal storage unit, the so-called *MW Database*.

Specific kinds of LMVRCS are *Billing Management Information Systems (BMIS)*, *Distribution Management System (DMS)*, *Energy Management System (EMS)*, an *Enterprise Service Bus (ESB)*, *Supervisory Control And Data Acquisition (SCADA)* systems, and *Substation Automation and Configuration Management (SACM)* systems. The MW communicates with the *Information Systems (IS)* of *Other Companies (OC)*, as well. OCs can be vendors or network providers.

All of the communications in the smart grid are two-way communications and form the so-called *Advanced Metering Infrastructure (AMI)*. This scenario is in alignment with other European projects regarding smart grids [14–17].

We use UML activity diagrams to model relevant behaviors for the target of analysis. For illustrative purposes we show in the following three examples of such diagrams.

We describe the so-called *Electricity SM Reading (for billing purposes)* process in Fig. 3. The SSN initiates the process every 24 hours (other time intervals are also configurable). The SM receives the request, queries its internal database and sends the results to the SSN. The SSN conducts validation and verification checks of the data. Validation checks are with respect to the data format of the transmission, for example to check whether the delivered values of the fields match their defined data types. Example

fields are current date, initial date of the measuring, voltage measured, and voltage interruptions during the billing period. An overview of all entry fields is given in Fig. 4.

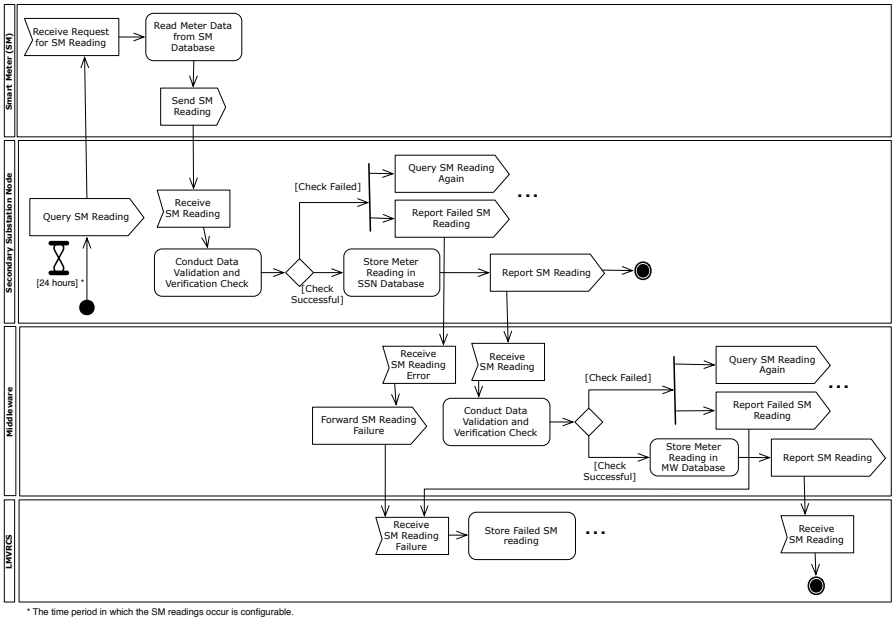

Fig. 3. Process Smart Meter Reading

The SSN also checks for verification errors of the data, for example to see if the consumer has a negative energy consumption. In the case that this customer is also an energy producer this might be possible, but for the consumers that are not this is a relevant check. If one of these checks fails the SSN sends a message to the MW and also asks the SM for another reading. We illustrate the repetition of the SM reading activities with three dots. If all checks of the reading are successful, the SSN reports the data to the MW and concludes the process. The MW forwards failed readings to the LVMRCS that stores the failed reading attempts. The correct readings the MW receives are checked again and if successful these are reported to the LVMRCS. If this is not the case the MW also reports a failed reading to the LVMRCS and initiates the reading process again. We abbreviate also this iteration with three dots. The LVMRCS moreover initiates actions to analyze the cause of the failed readings. For simplicity's sake, the details are not shown in this process and the remaining activities are abbreviated using three dots.

The data acquisition process illustrated in Fig. 5 begins with the LVMRCS inquiring SM reading data to the MW, which forwards the request to the SSN. The SM receives the request from the SSN and reads the metering data from its database. The data is

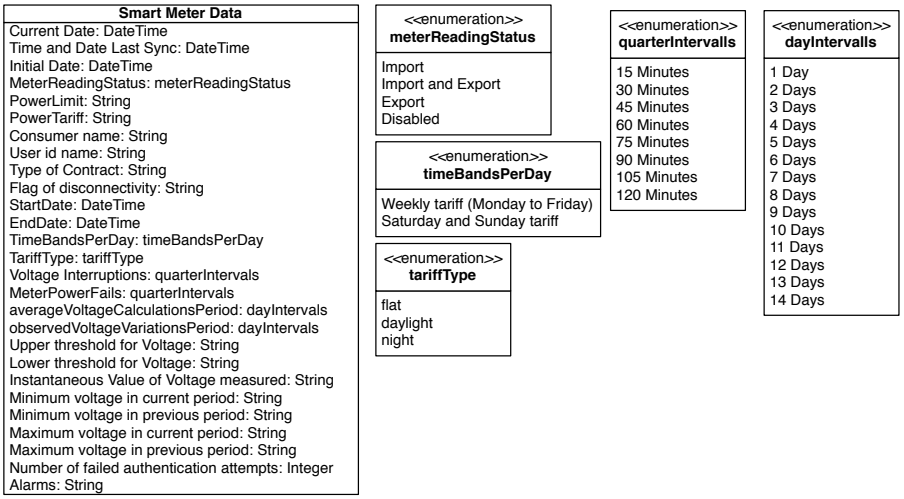

Fig. 4. Smart Meter Data Structure

sent to the SSN, from there to the MW, and finally to the LVMRCS. The validation and verification checks are conducted as described in the previous process. In case the LMVRCS receives a failed reading it initiates a failure analysis, which is abbreviated with three dots in the diagram.

The *Alarm and Event Management* process, depicted in Fig. 6, is concerned with constant error checks of each SM. The SSN initiates every 12 hours (the time period is configurable) a functionality check of the SM. The SM conducts a self-diagnostic after receiving this request. If the diagnostic is successful, the SM reports the success to the SSN and the process terminates. If the diagnostic reveals a problem, the SM retrieves its log information from the SM database and sends it in combination with the diagnostic to the SSN. If the SM does not reply within one hour (the time period is also configurable) a timeout occurs in the SSN. When either of these events occurs the SSN sends a notification of the problem to the MW. The MW analyses the received data and either issues a software update to the smart meter or reports the unsolved problem to the LMVRCS. The latter in turn initiates a failure analysis for the SM. This analysis is not shown in detail, but abbreviated with three dots in the diagram, because this is a process on its own.

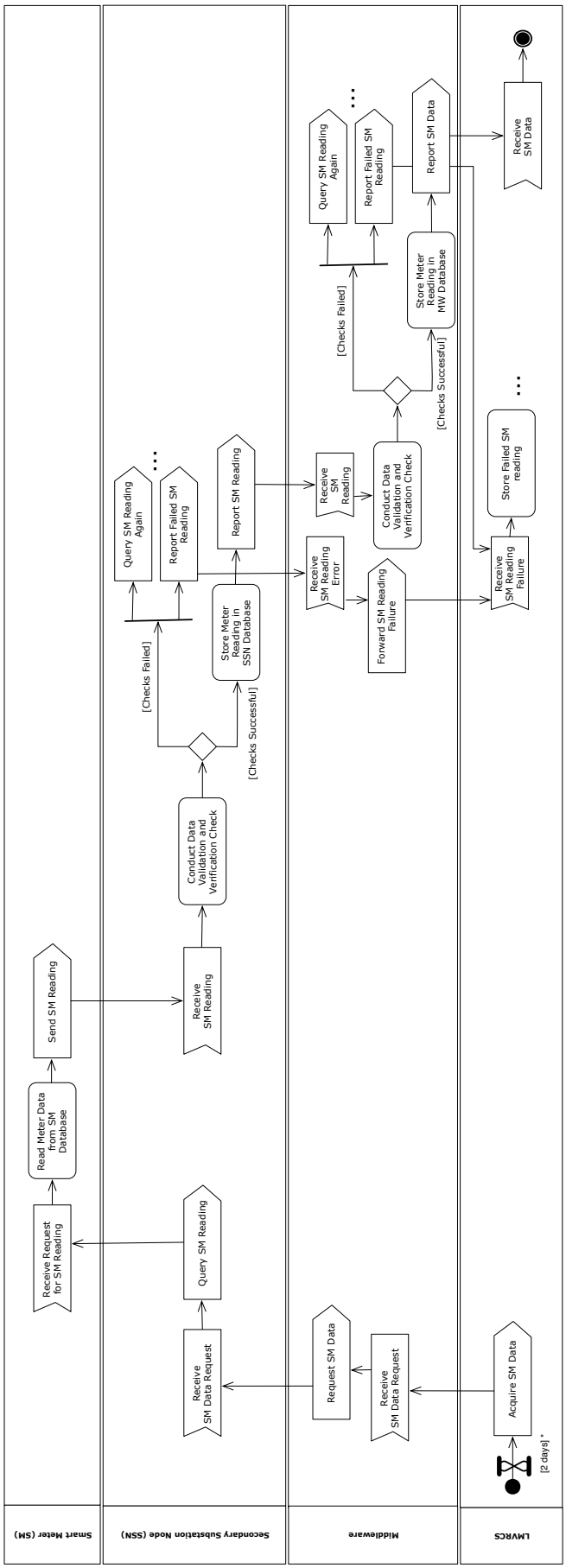

Fig. 5. Process Smart Meter Data Acquisition

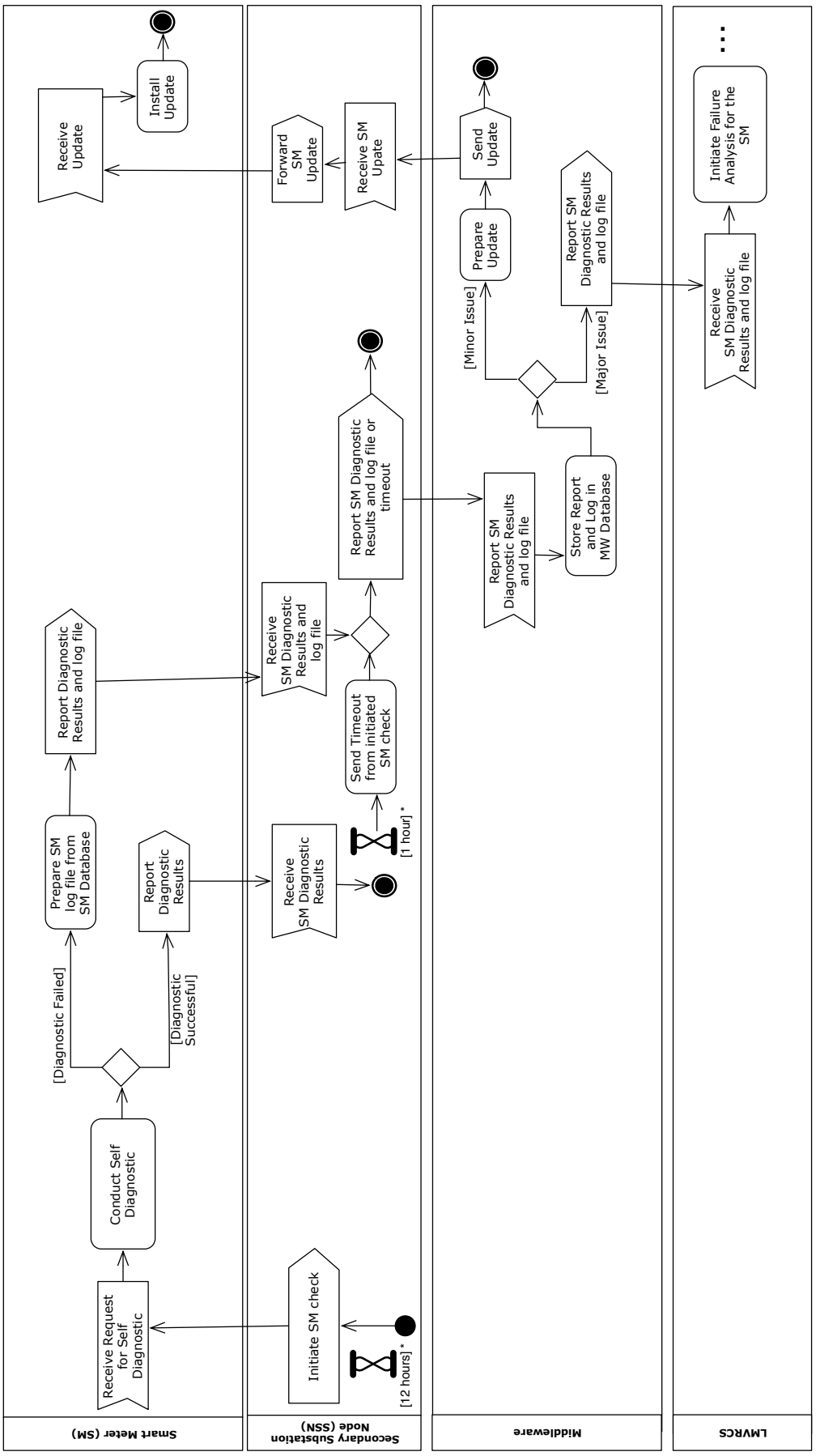

Fig. 6. Process Smart Meter Alarm and Event Management

The client (i.e. the commissioning party for this risk analysis) is the energy supplier, who conducts the study from the viewpoint of the consumers living in smart homes. The energy supplier is interested in analyzing privacy, integrity, and confidentiality concerns of consumers and how these can be assured by establishing an ISMS.

The energy supplier stated the following high-level security objectives:

- The integrity, confidentiality, and availability of consumers' configuration data of their home agents shall be preserved
- The privacy of the consumers' energy consumption data shall be preserved
- The integrity, confidentiality, and availability of the consumers' configuration data for their smart appliances shall be ensured

We state the exclusions from the scope in Tab. 2, based on the target description in Fig. 2 to Fig. 6.

Table 2. ISMS-CORAS scope exclusion table

Element of the Target Description	**Reason for Scope Exclusion**
Secondary Substation	The secondary substation is provided by the government and it is protected by the security team of the government
Secondary Substation Node (SSN)	The SSN is provided by the government and it is protected by the security team of the government
SSN Database	The SSN database is provided by the government and it is protected by the security team of the government
Middleware (MW)	The middleware has a Common Criteria certification
MW Database	The middleware database also has a Common Criteria certification
Information Systems (IS)	The middleware has a security testing policy in place to which all external ICT software has to comply
Other Company (OC)	The OCs have not a direct influence on the smart home as they only offer software services via their IS.
Energy Supplier	The energy supplier aims to create an ISMS to protect the consumers' security and privacy needs; hence, the energy supplier has not a harmful intent towards the consumers
Low/Medium Voltage Related Company Systems (LMVRCS) and all specializations of it	These are systems from the energy supplier that have passed a security certification

The assets in this scenario are depicted in Fig. 7 using a CORAS asset diagram. The *Consumers' Energy Consumption Data* shall be protected from attackers that use this data for creating behavioral profiles based on the consumption data. The value of the *Smart Appliances' Configuration* to the consumer is essential, because without it the consumer loses control about the appliances in their home. For example, a stove could heat up during the night and cause a fire. The *Home Agent's 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-to* relations; a relation from one asset to another means that harm to the former may lead to harm to the

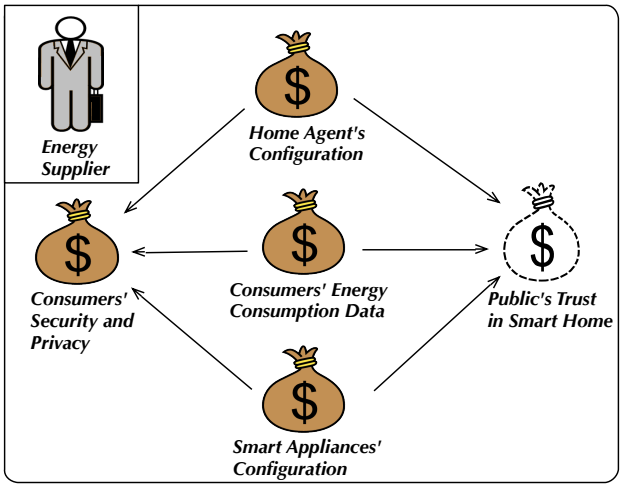

Fig. 7. Smart Home Asset Diagram

latter. Hence harm to the assets *Consumers' Energy Consumption Data*, the *Smart Appliances' Configuration*, the *Home Agent's Configuration* may cause harm to the overall *Consumers' Security and Privacy*.

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.

As a means to further focus the risk analysis, the assets are ranked according to their relative importance. This is shown in Tab. 3 where ranking 1 stands for very important and 5 stands for minor importance. The most important asset is the Consumers' Energy Consumption Data. The damage that a leakage of this information can cause to the consumer is significant, in particular because these may reveal behavior of persons in their homes. The smart appliances' configuration ranks second, because an incorrect configuration of an oven or a stove could cause a fire in the smart home. Less significant damages would be fridges that turn off such that the food inside it goes bad. When the configuration of the home agent is incorrect, this can cause financial loss due to the possibility of a too high price.

The asset table also has a column for stating the asset owner. We refer to the meaning of owner as defined in ISO 27001 Sect. 4.2.1.d (see Sect. 3), namely persons employed by the energy supplier that have management responsibly for considering the security concerns of a particular asset. Indirect assets do not have owners; the protection of these assets is assured via protecting the related direct assets.

Asset	Importance	Type	Owner
Consumers' Energy Consumption Data	1	Direct Asset	Mr. Jones
Smart Appliances' Configuration	2	Direct Asset	Mrs. Smith
Home Agent's Configuration	3	Direct Asset	Mr. Jones
Consumers' Security and Privacy	2	Direct Asset	Mrs. Jackson
Public's Trust in Smart Home	1	Indirect Asset	-

Table 3. Asset table with Asset Owners

We list existing controls for assets in Tab. 4. These refer to the controls implemented by the energy supplier. The supplier recommends also to choose security controls based on security standards. ISMS-CORAS supports this demand by using the ISO 27001 standard.

Asset	Existing control
Consumers' Energy Consumption Data	Secure communications between the SM and the SSN: Encrypted data communication and encryption of all data on removable devices like SD-cards. In addition, the data integrity is checked using certificates and hash values.
Smart Appliances' Configuration	None.
Home Agent's 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.
Consumers' Security and Privacy	All of the control listed above.

Table 4. Existing Controls Table

High-level Attacker Reasoning - This substep of the context establishment is concerned with narrowing down the number of possible attacker types for the defined target of analysis with its scope and focus. We reason about the unwanted incidents attacker types can cause and to which assets, and we document the assumptions and justifications for ruling out specific threats.[9] Moreover, we consider attacker motivations to sharpen the description of the proposed attackers.

This task uses three kinds of artifacts, namely attacker templates, attacker overview diagrams and a high-level risk table. The two first are ISMS-CORAS contributions, and the latter is extended to also capture the security objectives of the ISMS.

An attacker template (see Tab. 6) gives a structured way of describing attacker types, motivations, assumptions, and resulting threats via instantiating them. An attacker overview diagram is a graphical representation of an instantiated attacker template, and is used to give an overview of the attackers and to provide a basis for checking

[9] Note that in the CORAS terminology threats are attackers, persons, or other elements that are the initial cause of unwanted incidents. This is different from other terminologies in which threats are actual exploits of vulnerabilities. In this we mean that by the word threatened that an attacker causes an unwanted incident.

completeness of attacker identification. The information of all instantiated attacker templates and attacker overview diagrams serve as input for conducting a high-level risk analysis. The results are documented in the high-level risk table (see Tab. 10). This table shows *who* or *what* attacks a system, *how* the attack is conducted and the *harm* it causes. ISMS-CORAS extends the CORAS high-level risk table by a column that states the threatened *security objective* to a particular asset by that threat.

We have based our attacker templates and attacker overview diagrams on the ideas behind the work on misuse-cases as introduced by Sindre and Opdahl [18, 19]. Their work also relies on textual templates for describing misuse-cases that attackers conduct and corresponding UML use case diagrams [12]. The difference to our work is that ISMS-CORAS has a strong focus on security risk analysis, which is required for the compliance with the ISO 27001 standard. As depicted in Tab. 5 the attacker template consists of three parts, namely a *basic attacker description*, a *refined attacker description*, and a *results* part.

The basic attacker description starts with the definition of the attacker type, which is based on our previous work [20, 21]. This work classifies *Attacker*s 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., 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 the 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 Attacker*s 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 client also has to decide if the analyst shall only consider outside attackers or include inside attackers as well. Inside attackers are part of the system we analyze, while outside attackers are not. We propose this process of elimination of attacker types to allow the security and risk experts to focus on relevant threats of the target analysis, rather than considering every attacker type. The documentation moreover explains why certain attackers were not considered, which is useful for possible follow-up analyses after any system changes or changes in the security objectives.

Each of the attacker types should be considered in at least one of the instantiated attacker templates. This shall achieve a sense of completeness of the threat analysis. It is also possible to consider more than one attacker type in a template, e.g., when physical and network attacker are required for an attack. For simplicity's sake, we do not consider this case in our examples.

The usage of the template requires a statement about which assets are threatened by the attackers. The template has to be adjusted for each usage analysis, according to the assets shown in the asset diagram (see Fig. 7). Afterwards a task is to state which of the security goals of confidentiality, integrity, and availability that is/are threatened, and a reasoning of *why* assets and security goals are selected or ruled out. The reasoning should be based on the attacker type. For example, a network that is limited to the

physical boundaries of a building cannot be threatened by a network attacker outside the building. Another example is that a physical attacker can threaten the availability of a digital file, but this attacker type cannot threaten its integrity if the file exists in digital form and not in physical form.

We based the fields *entry points* and *attack paths* on Microsoft Threat Modeling [22]. This technique focuses on analyzing all interfaces of the target description elements to the outside world, so-called *entry points*, and afterwards analyzing how an attacker can reach a particular asset from this entry point. 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 attacker template is to identify assumptions about elements of the target description that reduce the number of entry points or attack paths. For example, if a network connection is embedded into a layer of concrete, an assumption could be that a physical attacker cannot reach this connection due to the significant effort required for penetrating the concrete.

The *refined attacker description* requires a description of the skills an attacker needs in order to succeed in harming the assets. For example, a network attacker might require skills to tamper with the network addresses of messages sent over a network. The field *attacker motivation* is based on a study from the SANS Institute[10] that revealed four fundamental motivations of social engineering attackers: *Financial gain*, *self-interest*, *revenge*, and *external pressure*. Financial gain means the attacker aims for monetary gain for various reasons. Self-interest could be the modification or destruction of information about a person with whom the attacker has a relation. Revenge is defined as the attacker's emotional desire for vengeance, for reasons only the attacker is aware of. This could, for example, be an attack on an employer or a competitor. External pressure towards an attacker occurs in different forms, e.g., friends, family or an organization force the attacker to satisfy their motivations for financial gain, self-interest, or revenge. We believe these motivations are generic enough to serve as basic types of attackers in the information system domain. We also added the motivation *curiosity*, which we identified in discussions with the industrial partners of the NESSoS project. Curiosity motivates an attacker to gain knowledge about the contents of a certain data set or simply to find out if his/her skills are sufficient to penetrate a system.

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. For example, the motivation *financial gain* does not make sense in regard to a physical attacker that only threatens the availability of information assets. Existing threat classifications (such as the STRIDE classification [23]) 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* state the kind of resources in terms of material and money the attacker requires to succeed in his/her attack. The instantiation of the template also

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

involves the elicitation of *assumptions about the attacker*. For example, the reason for a scope exclusion of a motivation can be an assumption that this motivation is not a concern of the customer. For example, a customer can state the attackers motivated by curiosity do not concern him/her, because this motivation may not lead to intentional damage of assets. 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.

The attacker overview diagrams (see Fig. 8) give a graphical overview of the identified attackers, and have two parts. The upper part of the diagram shows the assets that the attacker threatens, and which of the properties of confidentiality, integrity and/or availability that may be harmed. The lower part shows the elements of the target description that of an attacker can use to enter the system. The diagram also shows what assets are not threatened by the attacker and which elements of the target description are not entry points for the attacker. These assets and target description elements are positioned outside the frame of the attacker overview diagrams. Attacker overview diagrams always refer to a specific instantiation of an attacker template and represent some vital information of the template for security reasoning. These diagrams provide the basis for structured discussions about the validity of the elicited attackers. In addition, the documentation of the assets and target description elements supports the change management of the ISMS. All of these elements have to be re-evaluated after a change to the scope of the ISMS occurred and it has to be reasoned if they are still out of reach of the attacker.

We show instantiated attacker templates and attacker overview diagrams for physical attackers (see Tab. 6 and Fig. 8), for network attackers (see Tab. 7 and Fig. 9), for software attackers (see Tab. 8 and Fig. 10), and for social engineering attackers (see Tab. 9 and Fig. 11).

Table 5. 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.

Table 6. Attacker Template Instantiated for a Physical Attacker

Basic Attacker Description	
Attacker Type	⊠Physical Attacker □Network Attacker □Software Attacker □Social Engineering Attacker
Threatened Assets	⊠Home Agent's Configuration ⊠Consumers' Energy Consumption Data ⊠Smart Appliances' Configuration
Threatened Security Goals	⊠Availability □Confidentiality □Integrity
	Reasoning
	– The physical attacker threatens only the availability of the assets, because all of them are in electronic form. – The assets would need to have physical form for the attacker to read (threats to confidentiality) or change their content (threats to integrity). – The availability is threatened, because the attacker can destroy the SM, HA, and SA.
Entry Points	□SM □HA □SA □TH □ICTG □CHED □CO ⊠Smart Home
	Reasoning
	The physical attacker has to enter the smart home in order to threaten the availability
Attack Paths (possible vulnerabilities)	The physical attacker enters the smart home in order to destroy the SM, HA, and SA.
Assumptions of the Target Description	⊠SM □HA □SA □TH □ICTG □CHED □CO ⊠Smart Home
	The smart home is protected with at least two locks on the front door and when the consumers are not home all windows and doors are locked. In addition, it is envisioned that the smart home has an alarm system connected to the SM that reports unauthorized entries to the police.
Refined Attacker Description	
Required Attack Skills	Basic burglary skills
Attacker Motivation	□financial gain □self-interest ⊠revenge ⊠external pressure □curiosity
	Reasoning
	– The physical attacker cannot breach the confidentiality or integrity of the assets. This makes financial gain, self-interest, and curiosity unlikely motivations, because the attacker cannot sell information or change it in order to have a benefit, e.g., less payment for electricity. – The physical attackers are motivated by revenge or external pressure, which could motivate him/her to threaten the availability of the assets.
Required Resources	Basic burglary tools
Assumptions about the Attacker	We do not assume that an attacker is motivated by revenge, self-interest, or external-pressure to enter the home specifically for harming the smart home assets. We also assume that armed physical attackers that could force their way into the home at gunpoint do not specifically target the smart home assets. The reason is that these attackers would not risk getting caught just to harm the smart home assets. These would likely conduct kidnapping or burglary crimes.
Insider / Outsider	If the attacker is an insider, he/she does not have to breach the perimeter of the house. However, an attack would raise immediate suspicion if there are no signs of an external attacker.
Results	
Threats	A physical attacker can break into the smart home and destroy elements of the target system.
Reasons for Scope Exclusion	A highly skilled physical attacker might be able to manipulate the sensors of the SM to the extent that these provide wrong values for the energy consumption. However, the skills of such an attacker makes it unlikely to happen in a normal usage scenario. Hence, we exclude this attacker from the scenario.

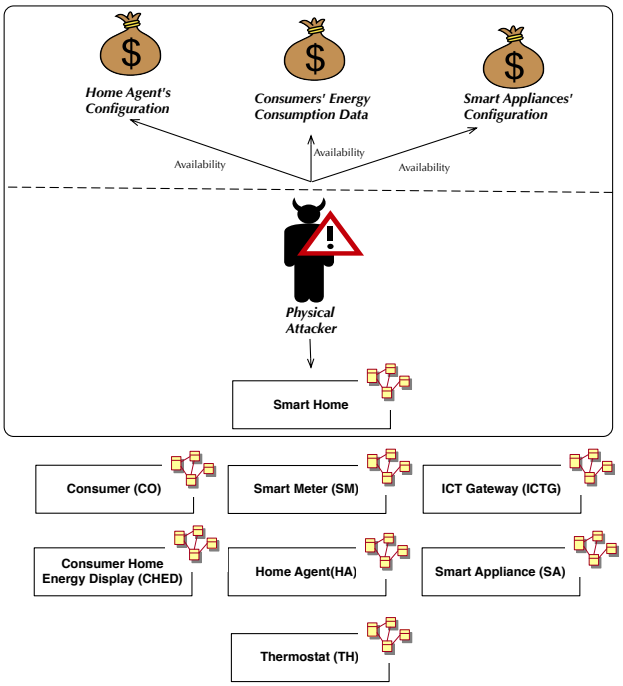

Fig. 8. Physical Attacker Overview Diagram

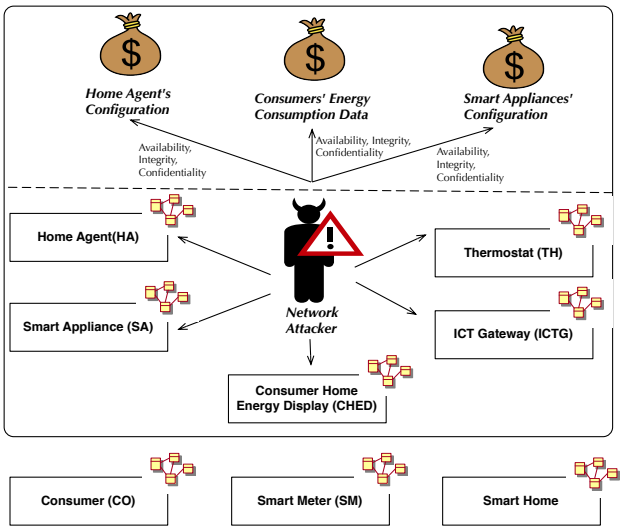

Fig. 9. Network Attacker Overview Diagram

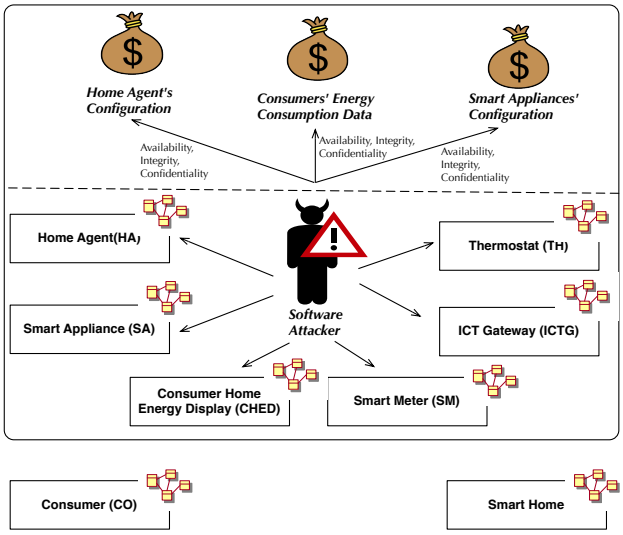

Fig. 10. Software Attacker Overview Diagram

Table 7. Attacker Template Instantiated for the Network Attacker

Basic Attacker Description	
Attacker Type	□Physical Attacker ⊠Network Attacker □Software Attacker □Social Engineering Attacker
Threatened Assets	⊠Home Agent's Configuration ⊠Consumers' Energy Consumption Data ⊠Smart Appliances' Configuration
Threatened Security Goals	⊠Availability ⊠Confidentiality ⊠Integrity
	Reasoning
	– The network attacker can use DoS attacks to reduce the availability of all network assets, e.g., send more message to the HA than it can process. – The network attacker can also read the network messages regarding energy consumption (breach of confidentiality) and even change them (threat to integrity). – The same can be said for the other assets if they are transferred over the network.
Entry Points	□SM ⊠HA ⊠SA ⊠TH ⊠ICTG ⊠CHED □CO □Smart Home
	Reasoning
	– The attacker can pretend to be a HA, TH, ICTG, or CHED in the network. – The SM cannot be impersonated, because of strong authentication mechanism. – The CO cannot be spoofed in the network, because it is a person. A similar argument goes for the smart home.
Attack Paths (possible vulnerabilities)	The network attacker can enter the network and pretend to be one of the network devices listed in the entry points and afterwards open a communication with any other device in the smart home.
Assumptions of the Target Description	⊠SM □HA □SA □TH ⊠ICTG ⊠CHED □CO □Smart Home
	We assume the consumer has a firewall installed that protects the ICTG from uninitiated connections with the internet. In addition, the sensor for measuring energy consumption is part of the SM. Hence, information for measuring energy consumption is not transmitted over the internal network of the smart home. Only the already measured energy consumption is transmitted between the SM and the CHED.
Refined Attacker Description	
Required Attack Skills	Network hacking skills
Attacker Motivation	□financial gain □self-interest ⊠revenge ⊠external pressure ⊠curiosity
	Reasoning
	– The attacker can conduct a revenge crime by making the energy consumption profile public or change the configuration of an SA that is a heater. – The attacker could turn the heater off in winter as a result of external pressure. – The attacker could also be curious about which SA he/she can remotely control, e.g., increase the temperature of a fridge to its maximum.
Required Resources	The attacker requires a computer with network access and probably a number of network attack tools.
Assumptions about the Attacker	We assume that the attacker in this scenario has just a basic skill set and that a correctly configured firewall will protect the system from an outside attacker. The inside attacker presents the important threat in this scenario.
Insider / Outsider	Outsiders have to pass the firewall of the consumer first. Thus, these have to have a greater skill set than internal attackers.
Results	
Threats	Spoofing and Tampering with the network messages. This can occur when the assets are transmitted over or via the network.
Reasons for Scope Exclusion	The network attacker from the outside with mediocre skill is excluded from the threat analysis.

Table 8. Attacker Template Instantiated with Software Attackers

Basic Attacker Description	
Attacker Type	□Physical Attacker □Network Attacker ⊠Software Attacker □Social Engineering Attacker
Threatened Assets	⊠Home Agent's Configuration ⊠Consumers' Energy Consumption Data ⊠Smart Appliances' Configuration
Threatened Security Goals	⊠Availability ⊠Confidentiality ⊠Integrity
	Reasoning
	– A software attacker could bypass the access control mechanism of the SM and threaten the asset Consumers' Energy Consumption Data. – The attacker could delete the software that runs on the meter (threats to availability), change the meter readings (threats to integrity), or read the meter reading (threats to confidentiality). – The attacker represents a similar threat to the other assets on the SA and HA.
Entry Points	⊠SM ⊠HA ⊠SA ⊠TH ⊠ICTG ⊠CHED □CO □Smart Home
	Reasoning
	– A software attacker could exploit vulnerabilities in the SM software, e.g., buffer overflow attacks to gain control of the SM. – The HA, SA, TH, ICTG use web interfaces for their configuration. – The software attacker could use, e.g., cross side scripting attacks to reduce the availability of these software systems. – The software attacker could also use, e.g., SQL injections to read and change the assets Home Agent's Configuration, and Smart Appliances' Configuration.
Attack Paths (possible vulnerabilities)	The attacker could compromise the ICTG and the TH first, and then use their connection to the HA or SA to read (threats to confidentiality) or change (threats to integrity) their configuration. Afterwards it could use the connection from HA or ICTG to attack the SM.
Assumptions of the Target Description	⊠SM ⊠HA □SA □TH ⊠ICTG □CHED ⊠CO □Smart Home
	We assume the SM does not have a direct communication/web-interface for the CO. The communication is guided via the HA or ICTG.
Refined Attacker Description	
Required Attack Skills	basic / advanced knowledge of software attacks
Attacker Motivation	⊠financial gain ⊠self-interest ⊠revenge ⊠external pressure ⊠curiosity
	Reasoning
	– The change in the energy consumption data could lead to financial gain for the attacker. – Self-interest could also protect other COs from spending money. – Revenge could be the intent to harm the CO by increasing the values for energy consumption in the smart grid. Revenge can also be to configure SAs to conduct attacks like creating a fire using a misconfiguration of the oven. – All of these threats could be motivated by external pressure, as well. – The reading and changing of energy consumption data could be motivated by curiosity, as well as the reconfiguration of SA and HA.
Required Resources	Computer with an interface to the SA, HA, ICTG, TH, and probably software hacking tools.
Assumptions about the Attacker	We assume that SA, HA, ICTG, TH have basic protection against attacks and that a certain skill level is required to attack them.
Insider / Outsider	Financial gain is unlikely for an outsider, because she/he does not participate in the energy consumption of the smart home. An exception of this could be that the attacker is collaborating with a physical attacker and the electricity line is compromised and energy is redirected to the outside attacker. The software attacker modifies the energy consumption in order for the CO not to recognize the attack. However, the physical connections that transport the electricity are unlikely to remain undetected in the smart home. Hence, we exclude this attack.
Results	
Threats	Software attacker can exploit the software of the SA, HA, ICTG, TH and manipulate their configuration and energy consumption. This could also lead to the use of SAs for attacks, reduce the availability of SM and cause the HA to negotiate a tariff that causes financial harm to the CO.
Reasons for Scope Exclusion	Outside attacker with a financial gain motivation or self-interest.

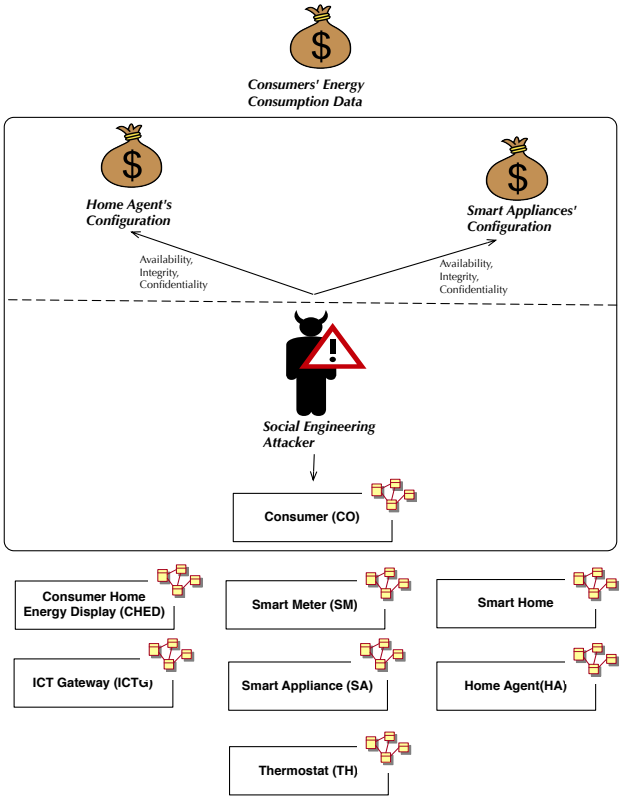

Fig. 11. Social Engineering Attacker Overview Diagram

Table 9. Attacker Template Instantiated with the Social Engineering Attacker

Basic Attacker Description	
Attacker Type	□Physical Attacker □Network Attacker □Software Attacker ⊠Social Engineering Attacker
Threatened Assets	⊠Home Agent's Configuration □Consumers' Energy Consumption Data ⊠Smart Appliances' Configuration
Threatened Security Goals	⊠Availability ⊠Confidentiality ⊠Integrity
	Reasoning
	– The social engineering attacker can manipulate humans in deleting (threats to availability), modifying (threats to integrity), or telling (threat to confidentiality) the configuration of SA and HA. However, the energy consumption data is stored in the SM and the CO does not have the access rights to change these. – They could tell the overall consumption, but since the CO does not tell all the details of the measurements, we consider the energy consumption secure from confidentiality, as well as availability threats.
Entry Points	□SM □HA □SA □TH □ICTG □CHED ⊠CO □Smart Home
	Reasoning
	– The only human the social engineering attacker can manipulate in this scenario is the CO.
Attack Paths (possible vulnerabilities)	The social engineering attacker contacts the CO and manipulates the person into deleting (threats to availability), modifying (threats to integrity), or telling (threat to confidentiality) the content of all the information assets.
Assumptions of the Target Description	□SM □HA □SA □TH □ICTG □CHED ⊠CO □Smart Home
	We assume the CO has not been trained to detect social engineering attackers. In addition, the CO has no strong mechanisms implemented to authenticate persons contacting him/her.
Refined Attacker Description	
Required Attack Skills	The attacker needs to be able to communicate with the CO and be able to pretend to be a person the CO can trust.
Attacker Motivation	□financial gain □self-interest ⊠revenge ⊠external pressure ⊠curiosity
	Reasoning
	– The social engineering attacker is not motivated by financial gain, because the CO is not able to change the metering data in the SM. – The social engineering attacker is not motivated by self-interest, because the manipulation of the configuration of SA and HA can only support other parties in the smart home marginally. – The social engineering can be motivated by revenge and cause the CO financial harm via misconfiguration by the HA or physical harm by misconfiguration of the SA, e.g., a fire caused by an overheating stove. – These acts can be motivated by external pressure as well. – The social engineering attacker can also be curious how the SAs and the HA is configured.
Required Resources	The social engineering attacker requires skills to pretend to be a person that the CO can trust. The attacker requires impersonation skills, e.g., the attacker can impersonate the technical support of the energy supplier.
Assumptions about the Attacker	We assume the CO only responds to reasonable requests of social engineering attackers. An example for an unreasonable effort would be to physical destroy the smart meter or an SA.
Insider / Outsider	Insiders are familiar with the behavior of the persons livening in the smart home and might be able to conduct the attack with less effort.
Results	
Threats	The social engineering attacker can impersonate persons the CO trusts, e.g., support employees of the energy supplier. This way the attacker can manipulate the CO to misconfigure SA or HA.
Reasons for Scope Exclusion	-

Validation Conditions - We propose to check the instantiations of the attacker template via several validation conditions. We have identified the following conditions so far:

- Check that all marked assets are threatened at least once by the attacker
- Check that the marked security goals are used at least once in relation to an asset
- Check that all selected motivations are reasoned about at least once
- Check that all unmarked security objectives, motivations, attacker types etc. are explained
- Check that the resources and the skills of the attacker are correct and that nothing is missing in the description explaining the full path for the cause of the unwanted incidents
- Check that all target description elements are covered by the templates
- Check that all assets are covered by the template
- Check that the high-level risk table refers to all threats stated in the instantiated templates

Conduct Customer Verification Review - The instantiated attacker templates and attacker overview diagrams have to be verified by the client. A meeting should check for completeness of the considered entry points and of the attack paths. These discussions should involve attacker models that rely on attackers' motivation, skills and resources.

In Tab. 10 we present an extended CORAS high-level risk table. We used the instantiated attack templates and template overview diagrams as input when creating the table. The column *what makes it possible* refers only to security vulnerabilities, because security is the focus of this paper. Please note that CORAS may address also other incidents and vulnerabilities, e.g., in relation to safety, which normally appear also in this column. Note also that in Tab. 10 we have not specified any specific security vulnerabilities, but for simplicity rather referred generically to the state of insufficient security.

Table 10. High-level risk table with security objectives

Who or what causes it?	How? What is the incident? What does it harm?	What makes it possible?	What are the security objectives?
Network Attacker	System break-in and theft of energy consumption data	Insufficient security	Confidentiality of energy consumption data
Network Attacker	System break-in and manipulation of smart appliances configuration data	Insufficient security	Availability of smart appliances, confidentiality and integrity of smart appliances' configuration data
Network Attacker	System break-in and manipulation of the home agents configuration	Insufficient security	Availability of the home agent, confidentiality and integrity of the home agent configuration data.
Software Attacker	System break-in and manipulation of energy consumption data	Insufficient security	Confidentiality, integrity, and availability of energy consumption data.
Software Attacker	System break-in and theft of energy consumption data	Insufficient security	Integrity of energy consumption data.
Software Attacker	System break-in and deletion of the smart meter software	Insufficient security	Availability of the smart meter
Software Attacker	System break-in and deletion of the smart appliances software	Insufficient security	Availability of smart appliances
Software Attacker	System break-in and deletion of the home agent software	Insufficient security	Availability of the home agent
Software Attacker	System break-in and configuring smart appliances to cause a fire or temperature drop in winter	Insufficient security	Integrity of smart appliances' configuration
Software Attacker	System break-in and misconfiguring of the home agent to increase the price of energy	Insufficient security	Integrity of home agent's configuration
Software Attacker	System break-in and configuring the CHED to display wrong energy consumption data	Insufficient security	Integrity of energy consumption data
Software Attacker	System break-in and configuring smart meter to delete the metering data	Insufficient security	Integrity of energy consumption data
Software Attacker	System break-in and configure smart appliance to raise a burglary alarm	Insufficient security	Integrity of smart appliances' configuration
Social Engineering Attacker	Manipulation of the consumer and deletion of home agent configuration	Insufficient security	Integrity of home agent's configuration
Social Engineering Attacker	Manipulation of the consumer to provide access to smart appliances	Insufficient security	Integrity of smart appliances' configuration
Social Engineering Attacker	Manipulation of the consumer to change the home agents configuration to buy only expensive energy	Insufficient security	integrity of home agent's configuration
Social Engineering Attacker	Manipulation of the consumer to remove the energy of the smart meter	Insufficient security	Availability of energy consumption data
Physical Attacker	System break-in and destruction of the smart meter	Insufficient security	Availability of energy consumption data
Physical Attacker	System break-in and destruction of the home agent	Insufficient security	Integrity of the home agent's configuration

A further important aspect of the context establishment step is the definition of scales for likelihoods and consequences, and the specification of the risk evaluation criteria.

Risk assessments can be conducted quantitatively or qualitatively. A quantitative risk assessment demands that the likelihood and consequence scales use numeric values. Because the system in our example is not yet fully built and deployed in a large scale yet, we express the likelihood and consequences using qualitative scales. Our likelihood scale is shown in Tab. 11 and the consequences in Tab. 12.

Table 11. Qualitative Likelihood scale for the Smart Home

Likelihood value	**Description**
Certain	A high number of similar incidents have been recorded; has been experienced a very high number of times by several consumers
Likely	A significant number of similar incidents have been recorded; has been experienced a significant number of times by several consumers
Possible	Several similar incidents on record; has been experienced more than once by the same consumer
Unlikely	Only very few similar events on record; has been experienced by few consumers
Rare	Never experienced by most consumers throughout the total lifetime of the Smart Home

Table 12. Qualitative Consequence Scale for the Smart Home

Consequence	**Generic interpretation**
Catastrophic	Can potentially put the energy supplier out of business
Major	Failure to recover can potentially put the energy supplier out of business
Moderate	Several occurrences over time can potentially put the energy supplier out of business
Minor	Tolerable if easy to recover from and if very rare
Insignificant	Generally tolerable and easy to manage to recover from

We use these scales for all assets, and we use the risk evaluation criteria specified by the matrix in Tab. 13. The matrix shows the acceptable combinations of likelihoods and consequences in light shading, and unacceptable combinations in dark shading.

Relevant Legal Aspects - The smart home scenario involves certain legal issues. We consider the German law, because our consumer and energy supplier are in Germany.

Germany's Energy Industry Act (EnWG) Sect. 21b Paragraph 3a states that all new buildings, as well as newly renovated ones, have to use smart meters. In addition, the network operators have to provide a smart meter to all consumers that request one. The network operators can provide these themselves or hire a third party to do so. Moreover, Sect. 40 of the EnWG states that energy suppliers have to offer energy tariffs that provide incentives for guiding or reducing energy consumption. These are so-called *load variable and daytime dependent tariffs*.

The principles of data avoidance and data minimization in German Federal Data Protection Act (BDSG) Sect. 3a prevent the collection of energy consumption data with-

Table 13. Risk evaluation matrix

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

out a valid reason[11]. The energy provider has such reasons, which are billing purposes. The consumer and the energy provider in our example have a tariff that requires the meter reading every day.

The EU and Germany envision that meter readings could occur in very small time intervals. The readings are transmitted to the energy provider. The smallest transmission interval is assumed to be 15 minutes [24–26]. These transmissions sum up to 35 040 transmissions of energy values a year. In our example, we assume transmissions of meter readings once a day, which sums up to 365 data transmissions a year.

Before the introduction of smart meters, the energy data was transmitted only once a year. In addition, the transmission contained only one value, which was the sum of the overall energy consumption at the time of the meter reading. The usage of smart meters allows the measuring of energy consumption every second, and storing it in a separate value. Thus, the transmission of energy data every 15 minutes can contain up to 900 different values. To sum up, the intervals in between energy data transmissions and the values this data contains increases significantly with the introduction of smart meters from previously one transmission with exactly one value once a year to hundreds or thousands of transmissions a year with at least that many values (if not more) in each transmission.

Metering data are personal data according to BDSG Sect. 1 Paragraph 2 and Sect. 3 Paragraph 1 because these provide information about the personal and factual living conditions of the consumers [25, 26]. Moreover, the BDSG Sect. 4 Paragraph 2 states that personal information has to be collected with the *involvement of the concerned person*, which in our example is the consumer. Hence, the consumer has to provide the energy consumption data and not the other way around. Mechanical meters have to be read by a person, which is often the consumer itself or a technician of the energy supplier. Either the consumer reads the value and transmits it to the energy supplier and, thus, the involvement of the concerned person (the consumer) can be assumed. Or the concerned person permits the technician access to the meter, which also implies the involvement of the concerned person. In both cases BDSG Sect. 4 Paragraph 2 is satisfied.

[11] The BDSG refers to personal information and according to [24–26] energy consumption data is personal information

However, the situation changes if a smart meter transmits meter readings automatically to the energy supplier and the consumer is not aware of it. In this case, the involvement of the concerned person (the consumer) cannot be assumed. This is a compliance problem with BDSG Sect. 4 Paragraph 2, but legal experts (see [25, 26]) argue that a large number of data transmissions causes an unacceptable effort for the concerned person. In our example this means 365 data transmissions a year (and up to 35 040 transmissions in other scenarios). Hence, the legal experts argue that if the concerned person (the consumer) provides an *informed consent* as described in BDSG Sect. 4 Paragraph 1, the energy provider is allowed to initiate the transmissions of the energy consumption data in compliance with the BDSG [25, 26]. BDSG Sect. 4 Paragraph 1 states that the collection, processing, or usage of personal information requires an informed consent of the concerned person. An informed consent requires that the concerned person is in possession of all the facts, implications, and future consequences of an action. In addition, the facts, implications, and future consequences have to be understood entirely and in every detail at the time consent is given [26].

Moreover, the collection of energy consumption data requires a legal contract between the energy supplier and the consumer to be in compliance with BDSG Sect. 28 Paragraph 1 Nr. 1. The contract has to specify in which intervals data is collected, the type of data collected, and the time frames when the data is collected and how the documentation of the stored data. The data also can only be used for the purpose it is collected [26].

The collection, processing, or distribution of energy consumption data requires an informed consent in compliance with BDSG Sect. 4 Paragraph 1 (see above). If energy data is collected from an energy provider (or any other stakeholder) without an informed consent, even though the technical means in smart meters exist, this is a misdemeanor according to BDSG Sect. 43 Paragraph 2 Nr. 1. This misdemeanor can result in a maximum fee of 300.000 Euro in Germany (see [26]). In addition, BDSG Sect. 7 provides the basis for the consumer to claim compensation for damages and defects [26].

In our example, a default configuration of a smart meter that collects energy data in 15 minutes intervals would be a violation of the BDSG, because the energy provider has only the informed consent of the consumer to collect the energy consumption once every day, and the transmitted value is supposed to be just the sum of the energy consumption of the consumer of each day. Every other data collected is a violation of the BDSG and is punishable by the fines stated above.

We describe a legal consequence scale for the smart home scenario in Tab. 14. The scale is concerned with compliance with data protection laws and regulations, which in our scenario is particularly related to the Consumers' Security and Privacy. We introduce the asset of compliance with governmental laws and regulations, using the short name *Legal Compliance* for the asset for the remainder of the report.

Given our target of analysis, legal compliance issues are mostly relevant to incidents related to consumers' security and privacy. Nevertheless, by introducing legal compliance as an asset of its own, we make the legal risks explicit in the analysis and in the documentation of the results. Note that for the consequence scale in Tab. 14, each consequence typically includes all lower consequences, as the legal consequences with

respect to this asset usually escalate. We use the risk matrix in Tab. 13 as the evaluation criteria for compliance also.

Table 14. Qualitative Legal Consequence Scale for the Smart Home

Consequence	Generic interpretation
Catastrophic	Processing of personal data ordered to cease
Major	Civil law liability and fine; criminal law liability and prison sentence
Moderate	Enforcement notice
Minor	Information notice
Insignificant	Minor breach of consumer's privacy discovered and corrected

4.2 Step 2: Identify Risk

The risk identification refines the attacker descriptions in the high level risk table into threat diagrams. These show the detailed attack paths of attackers into the system, and how an unwanted incident may be caused. CORAS makes use of workshops, structured brainstorming and other techniques to elicit unwanted incidents and describe the scenarios that may lead to them.

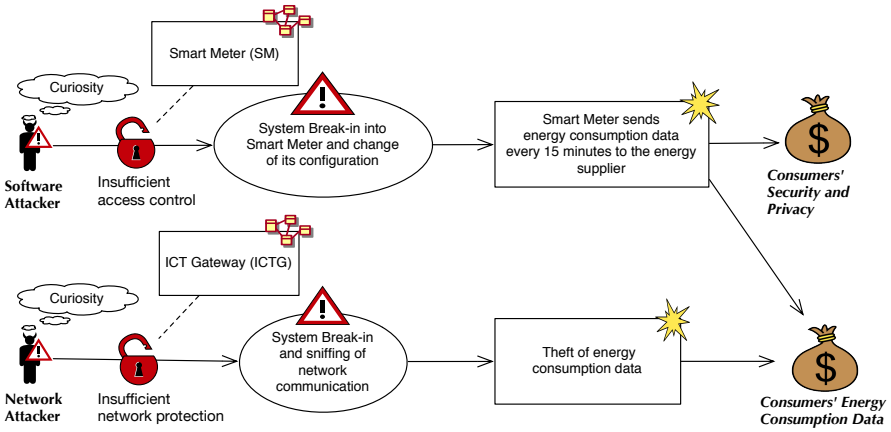

Fig. 12. Extended Threat Diagram for Software and Network Attacker

We show a small example threat diagram in Fig. 12 to illustrate how ISMS-CORAS extends the CORAS threat diagram notation. One extension is the attacker motivation, depicted as clouds over the attacker symbol. We consider a software attacker and a network attacker in our example. Another extension is the relation from a vulnerability to the element of the target description that contains the vulnerability. In our example, a

software attacker exploits the vulnerability ”insufficient access control”, which is contained in the smart meter. The threat scenario is that the attacker breaks into the smart meter and changes the configuration. The software attacker is not trying to enrich her-/himself, because the motivation is ”curiosity”. The attacker changes the smart meter configuration in such a way that the meter sends the energy consumption data to the energy supplier every 15 minutes.

The network attacker has the same motivation and exploits the ”insufficient network protection” vulnerability, which is contained in the ICT Gateway. The unwanted incident is a theft of the energy consumption data.

We show the extended threat diagram notation that uses Legal CORAS in in Fig. 13. In our example scenario the German Federal Data Act (BDSG) applies, because the energy consumption data of the consumer is considered personal data, and because the sending of energy consumption data in shorter intervals than the tariff requires without the consumers informed consent is a violation of BDSG Sect. 4. The energy supplier is therefore subject to the risk of getting fined or sued, due to liability. This can cause the unwanted event of prosecution of the energy supplier for storing and processing of personal information without an informed consent. The law suit can result in a fine of up to 300.000 Euro [26]. Given our scale of legal consequences, such a fine could correspond to a consequence up to “major”.

4.3 Step 3: Estimate Risk

Step 3 and Step 4 remain almost unchanged from CORAS, and we therefore describe this part more briefly. In Step 3 the likelihoods and consequences are estimated and discussed with the customer, and the results are annotated in the threat diagram using the scales introduced previously. The annotated threat diagram, including the legal uncertainty, is depicted in Fig. 14.

The system break-in of the software attacker has the likelihood “possible”, due to the existing vulnerability “insufficient access control”. The resulting unwanted incident is assigned a major consequence for the asset *Consumers' Security and Privacy*, because the energy provider gains more details about the consumers' energy consumption, and could also derive behavioral profiles of the consumers. This is moreover in violation of the BDSG. As depicted by the legal norm in Fig. 14, it is held as “possible” that that this norm applies to these circumstances. Consequently, it is held as “possible” that the incident of legal prosecution occurs. The legal consequence with respect to compliance is estimated to be “moderate”.

Similar reasoning is conducted to estimate the risks with respect to the consumers' energy consumption data. The consequence of consumption data readings every 15 minutes is held as “minor” since misuse by the energy supplier is not assumed. The consequence of theft of energy consumption data is, however, held as “major”, because the data could be used to analyze the behavioral profiles of the customer and used, for example, to commit burglaries when the consumer is not likely to be at home.

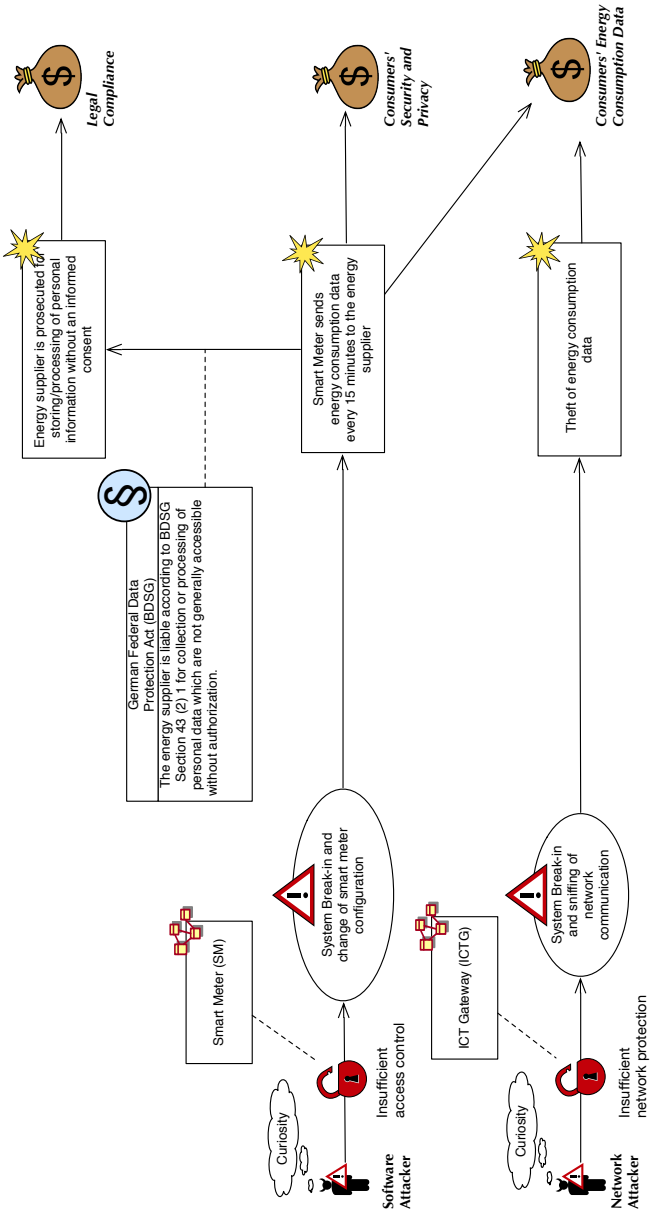

Fig. 13. Extended Threat Diagram notation for Software and Network Attacker including Legal Concerns

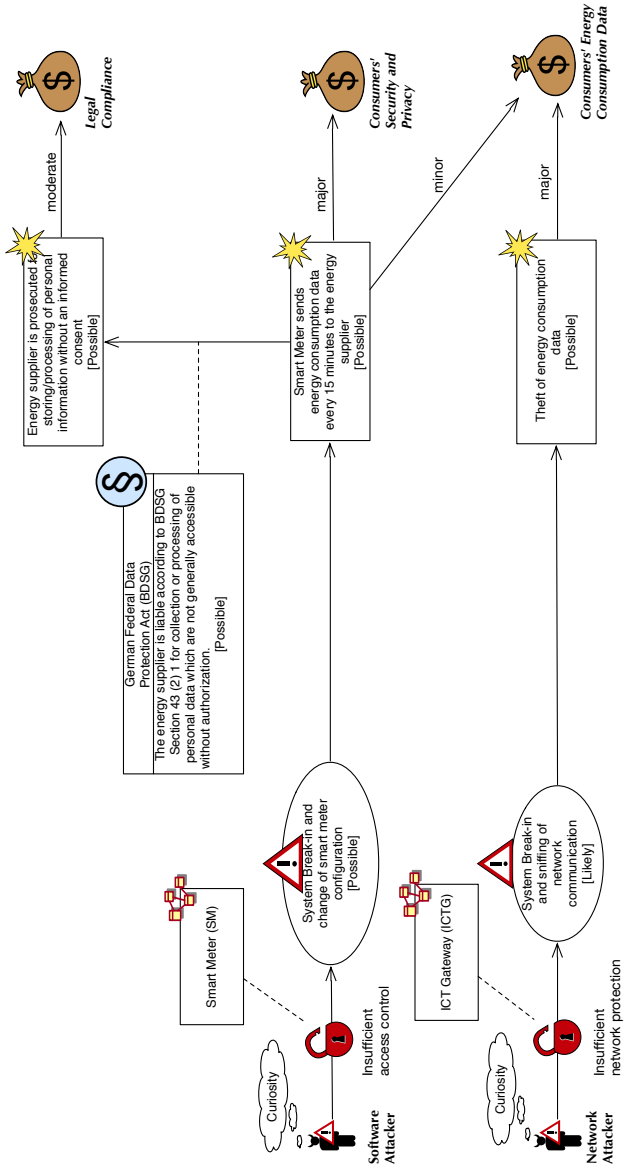

Fig. 14. Extended Threat Diagram for Software and Network Attacker including Legal Concerns

4.4 Step 4: Evaluate Risk

The values for consequences and likelihoods of unwanted incidents as estimated in the previous step are combined into risks and drawn in risk diagrams (see Fig. 15). The values for likelihoods and consequences are plotted into the risk matrix, depicted in Tab. 15. The matrix determines whether a risk is acceptable or should be considered for treatment, which is conducted in the next step.

As depicted in Fig. 15, the software attacker gives rise to three risks. The risk *PP* states that the energy supplier can be prosecuted for storing or processing of personal information without an informed consent, and is assessed as unacceptable. The situation is similar for the *SMS 1* risk, which consists of sending energy consumption data every 15 minutes to the energy supplier. The risk *SMS 2* on the other hand is acceptable due to the low consequence. Similarly, the *TED* risk is also categorized as unacceptable (see Tab. 15).

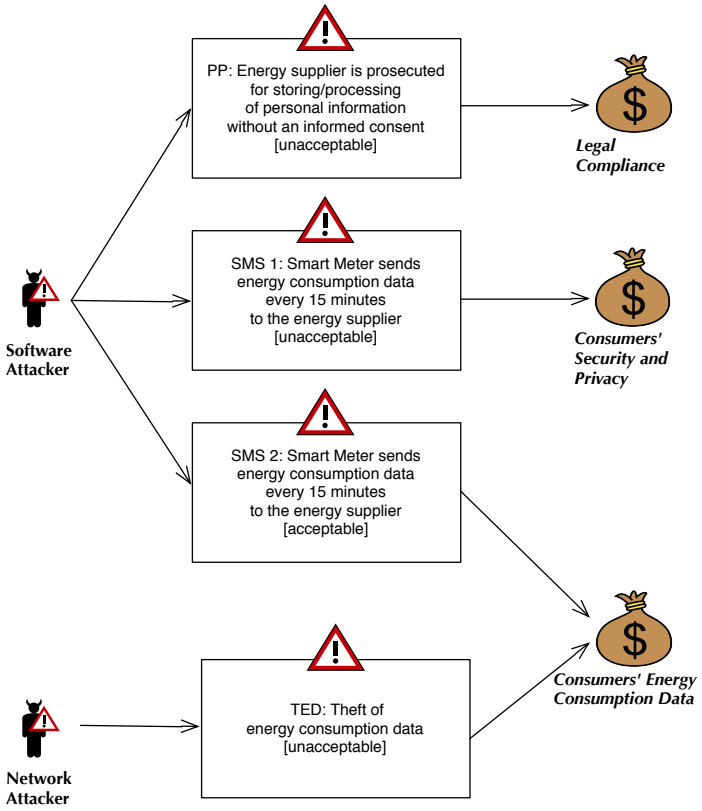

Fig. 15. Risk Diagram

Table 15. Risk evaluation using the risk matrix

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

4.5 Step 5: Treat Risk

The unacceptable risks have to be evaluated for possible treatment. Appendix A of the ISO 27001 standard describes the normative controls of the standard, and ISMS-CORAS requires these to be considered. We present a short overview of these controls in Tab. 16. The numbering of the controls starts with A.5 and ends with A.15 because this is the numbering used in the standard. The standard provides guidelines on how to implement these and other controls, but the implementation is not normative.

Table 16: Controls of the ISO 27001 Standard

Control Name	Control Objective	Important Demands
A.5 Security policy	Provide directions for information security	Documentation and Review Requirements
A.6 Organization of information security	Manage security within the organization and with external parties	Clear management commitment, responsibilities, coordination, and independent consultation and review
A.7 Asset management	Achieve and ensure appropriate protection levels for assets	Identify assets, assign responsibilities for assets, classify assets, define and document rules for treatment of assets
A.8 Human resources security	Provide security training for employees, communicate responsibilities, provide structured exit procedures	Specify role and terms of employment, define responsibilities and provide security education and training, define disciplinary process, define termination responsibilities, return of assets and removal of rights
A.9 Physical and environmental security	Prevent unauthorized physical access, damage and interference to secure areas and equipment	Establish security perimeter, physical controls for access to secure rooms. Equipment shall be protected e.g. from power failure and the support for the equipment shall be ensured e.g. protect cable connection from interference.

Continued on next page

Table 16 – continued from previous page

Control Name	Control Objective	Important Demands
A.10 Communications and operations management	Ensure secure operations of information processing, especially for service delivery from third parties, ensure availability, integrity, and confidentiality of information processing	Guidelines for processes, e.g., segregation of duties, and specific demand that ensure the goals e.g. back up and monitoring of processes
A.11 Access Control	Control the access to information	Ensure access control on information systems, networks, operating systems etc.
A.12 Information systems acquisition, development and maintenance	Embed security in information systems and prevent misuse of information	Specific measure are demanded e.g. security requirements analysis, input/output data validation, use of cryptography, prevent information leakage, etc.
A.13 Information security incident management	Identify security events and weaknesses associated with information security and provide timely corrective action, ensure a consistent and effective approach	Ensure a reporting for security events and security weaknesses, learn from information security incidents
A.14 Business continuity management	Protect critical business processes from effects of information system failures and ensure their timely resumption	Include security and risk management in the business continuity management process, reassess and test the business continuity plans
A.15 Compliance	Ensure compliance with laws, regulations, contractual obligations, security requirements, organizational security policies, and standards, consider system audits	Identify relevant laws, regulations, contractual obligations, etc. and also data and privacy protection measures, check the compliance to these laws, regulations, contractual obligations, etc. and use also audits to check compliance

We support the selection of controls with a mapping of controls to attacker types in Tab. 17. The table lists the controls and the attacker types whose threats can be mitigated by these controls. In addition, we list the control objectives and the types of target description elements that can be protected by these controls. Considering the information in our enhanced threat diagrams in combination with this table, the control selection should become more time efficient. In addition, ruling out a particular control for a specific attacker based on this table narrows down the choices for relevant controls to treat the risk.

For example, the software attacker in Fig. 14 has the motivation *curiosity*, exploits the vulnerability *insufficient access control* and the concerned target description element

is the *smart meter*. Using Tab. 17 we see that the control A.11 concerns *access control* and the attacker type *software attacker*, and the relevant target description elements are software. Thus, this control is of relevance for mitigating the particular threat described in Fig. 14, which is caused by the software attacker. We select relevant sub-controls of A.11 in our risk treatments, and proceed for the network attacker in a similar manner.

Table 17: Mapping Controls of the ISO 27001 Standard to our Attacker Types

Control Name	**Attacker Types**	**Control objective**	**Relevant Target Elements**
A.5 Security policy	All	Provide directions for information security	All
A.5.1.1 Information security policy document	All	Get approval by management, and publish and communicate to all relevant parties.	All
A.5.1.2 Review of the information security policy	All	Review and improve the policy continuously.	All
A.6 Organization of information security	All	Security management activity e.g. clear management commitment	All
A.6.1 Internal organization	All	Manage information security within the organization	All
A.6.2 External parties	All	Maintain the security of the organization's information and information processing facilities	All
A.7 Asset management	All	Activities regarding identify, classify and protect assets	All
A.7.1 Responsibility for assets	All	Achieve and maintain appropriate protection of organizational assets	All
A.7.2 Information classification	All	Ensure that information receives an appropriate level of protection	All
A.8 Human resources security	Social engineering attacker	Activities regarding training, responsibility assignment, designing and implementing exit procedures etc.	All that are humans
A.8.1 Prior to employment	Social engineering attacker	Ensure that employees, contractors and third party users understand their responsibilities	All that are humans
A.8.2 During employment	Social engineering attacker	Ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities	All that are humans
A.8.3 Termination or change of employment	Social engineering attacker	Ensure that employees, contractors and third party users exit an organization or change employment	All that are humans

Continued on next page

Table 17 – continued from previous page

Control Name	Attacker Type	Control objective	Relevant Target Elements
A.9 Physical and environmental security	Physical attacker	Activities regarding concerning physical access and prevention of damage/interference of hardware	All that are physical e.g. hardware
A.9.1 Secure areas	Physical attacker	Prevent unauthorized physical access, damage and interference	All that are physical e.g. hardware
A.9.2 Equipment security	Physical attacker	Prevent loss, damage, theft or compromise of assets	All that are physical e.g. hardware
A.10 Communications and operations management	All	Activities regarding guidelines for processes, e.g., segregation of duties	All
A.10.1 Operational procedures and responsibilities	All	Ensure the correct and secure operation of information processing facilities	All
A.10.2 Third party service delivery management	All	Implement and maintain the appropriate level of information security	All
A.10.3 System planning and acceptance	All	Minimize the risk of systems failure	All
A.10.4 Protection against malicious and mobile code	Software attacker	Protect the integrity of software and information	All that are software
A.10.5 Back-up	All	Maintain the integrity and availability of information and information processing facilities	All that are information or software
A.10.6 Network security management	Network attacker	Ensure the protection of information in networks	All that are part of the network
A.10.7 Media handling	All	Prevent unauthorized disclosure, modification, removal or destruction of assets	All that are media
A.10.8 Exchange of information	All	Maintain the security of information and software exchanged within an organization	All
A.10.9 Electronic commerce services		Maintain the security of information and software exchanged within an organization	

Continued on next page

Table 17 – continued from previous page

Control Name	Attacker Type	Control objective	Relevant Target Elements
A.10.10 Monitoring	Software attacker, network attacker	Ensure the security of electronic commerce services	All that are electronic commerce services
A.11 Access Control	Software-attacker/network attacker/physical attacker	Activities regarding implement and monitor access to information	All that are software
A.11.1 Business requirement for access control	All	Control access to information.	All
A.11.2 User access management	All	Ensure authorized user access	All
A.11.3 User responsibilities	All	Prevent unauthorized user access	All
A.11.4 Network access control	Network attacker, software attacker	Prevent unauthorized access to networked services	All that are part of the network or a networked service
A.11.5 Operating system access control	Software attacker, social engineering attacker	Prevent unauthorized access to operating systems.	All operating systems or in relation to operating system security
A.11.6 Application and information access control	Software attackers	Prevent unauthorized access to information held in application systems	Applications or in relation to application security
A.11.7 Mobile computing and teleworking	Software attacker, network attacker	Ensure information security when using mobile computing	All that are mobile computing or teleworking
A.12 Information systems acquisition, development and maintenance	Software-attacker/network attacker	Activities regarding eliciting of security requirements and vulnerability detection e.g. penetration testing and specific measures e.g. cryptography	All that are software or network components
A.12.1 Security requirements of information systems	All	Ensure that security is an integral part of information systems	All
A.12.2 Correct processing in applications	Software attacker	Prevent errors, loss, unauthorized modification	All applications
A.12.3 Cryptographic controls	Software and network attacker	Protect the confidentiality, authenticity or integrity of information	All applications and networks

Continued on next page

Table 17 – continued from previous page

Control Name	Attacker Type	Control objective	Relevant Target Elements
A.12.4 Security of system files	Software attacker, social engineering attacker	Ensure the security of system files.	All that are applications
A.12.5 Security in development and support processes	All	Maintain the security of application system software and information.	All
A.12.6 Technical Vulnerability Management	Software attacker, network attacker	Reduce risks resulting from exploitation of published technical vulnerabilities	All that are technical
A.13 Information security incident management	All	Activities regarding reporting security events and issues, ensuring a consistent and effective response, learning from security incidents,	All
A.13.1 Reporting information security events and weaknesses	All	Ensure information security events and weaknesses associated with information systems are communicated	All
A.13.2 Management of information security incidents and improvements	All	Ensure a consistent and effective approach is applied to the management of information security incidents.	All
A.14 Business continuity management	All	Activities regarding business continuity management for business processes e.g. security and risk management	All
A.14.1 Information security aspects of business continuity management	All	Counteract interruptions to business activities	All
A.15 Compliance	All	Activities regarding identifying laws, regulations and contractual obligations. privacy protection, monitor compliance to the laws regulations and contractual obligations, compliance audits	All
A.15.1 Compliance with legal requirements	All	Avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements	All

Continued on next page

Table 17 – continued from previous page

Control Name	Attacker Type	Control objective	Relevant Target Elements
A.15.2 Compliance with security policies and standards, and technical compliance	All	Ensure compliance of systems with organizational security policies and standards	All

We illustrate the selection of controls using our extended CORAS treatment diagram notation. These diagrams are used for identifying and documenting risk treatments, and the novelty of ISMS-CORAS is that the risk treatment and the diagrams have to consider ISO 27001 controls. Additionally, the attacker types and related target elements are specified as for threat diagrams.

In the example depicted in Fig. 16, we have identified treatments for the risks PP and SMS, which are caused by a software attacker. We can reduce a risk with controls to reduce its likelihood or consequence (or both). First, we select a control to reduce the likelihood of both risks. The risks PP and SMS are caused by the vulnerability insufficient access control. We select the control *A 11.2.4 Review of User Access Rights*, because an analysis of this issue resulted in the conclusion that the smart meter did not restrict access to the configuration for any user. In addition, we select *A12.6.1 Control of technical Vulnerabilities*, which reduces the likelihood of the existence of technical vulnerabilities that allow software attackers to change the access control rules established with the control A 11.2.4.

Second, we select controls to reduce the risk PP. This is of particular relevance, because in case the unwanted incident of sending energy consumption data in short intervals happens, a law suit is a possibility. The likelihood of this event cannot be influenced further with reasonable effort. Hence, it is important to reduce the possible consequence of such a lawsuit. The controls *A 10.10.5 Fault Logging* and *A 13.2.3 Collection of Evidence* are selected to reduce the consequences of the risk PP. Both controls aim to document the occurrences of the incident with the purpose of proving that the violation of the privacy of the consumer was not intended by the energy supplier. Hence, the legal sentence (the consequence) should be reduced. The risks SMS 1 and SMS 2 are only reduced via their likelihoods.

A focused view on only the risks and the selected controls is provided in the treatment overview diagram shown in Fig. 17.

We illustrate the selected controls for the TED risk in Fig. 18, which concerns the theft of energy consumption data caused by a network attacker. In this diagram, one element of the target description has to be protected, namely the ICT gateway. The vulnerability that has to be addressed by the controls is insufficient network protection. We identified the controls *A 11.4.6 Network Connection Control* and *A 11.4.2 User Authentication for External Connections* as relevant, because the controls restrict the access to certain network devices and implements strong authentication mechanisms. The control restrictions to the network refer to the ICT Gateway, while the authentication mechanisms refer to the Smart Meter. Moreover, the control *A 12.5.4 Information*

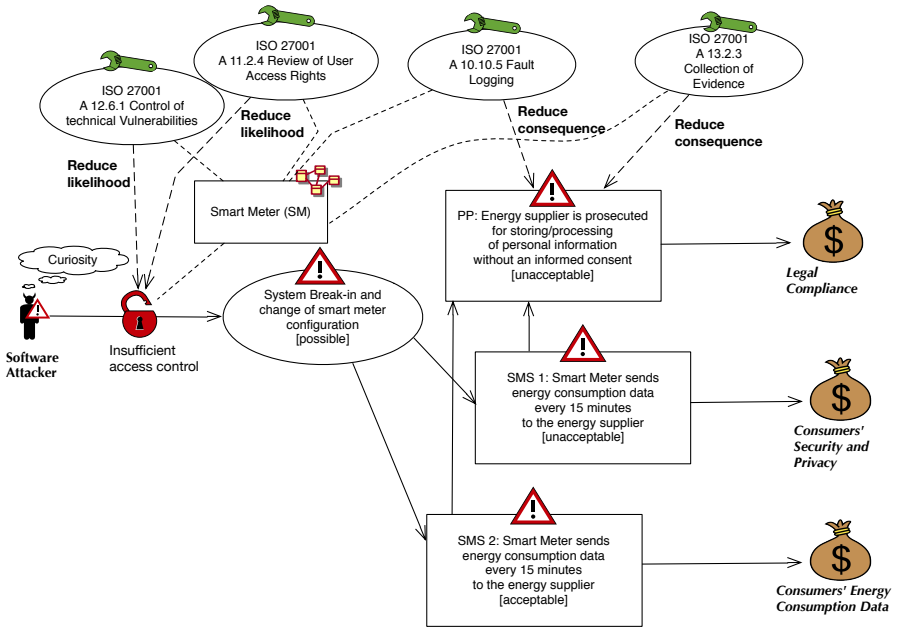

Fig. 16. Treatment Diagram I

Leakage Control shall reduce the likelihood of loss of energy consumption data from the ICT Gateway. The consequences of the TED shall be reduced with the control *A 13.2.2 Learning from Information Security incidents*. The control shall show that the energy provider will investigate every incident and learn from his/her mistakes. This shall result in improved controls and prevent the same exploit to happen twice.

A focused view on only the risk TED and the selected controls is provided in a treatment overview diagram, shown in Fig. 19.

We present all selected treatments in Tab. 18, which is a so-called treatment overview table. The first column shows the assets that shall be protected by the control. The second column shows the asset owner, who is responsible for implementing the control. The column is filled with made up names for illustrative purposes. The following columns state the addressed security objective, the selected treatment or control and the reason for selecting the control.

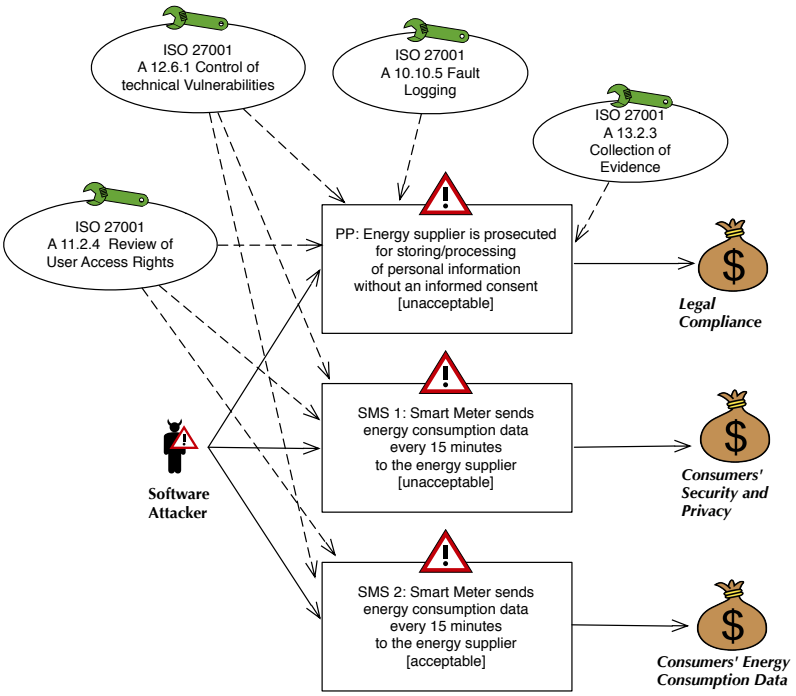

Fig. 17. Treatment Overview Diagram I

Table 18: Treatment Overview Table

Asset	**Asset owner**	**Security objective**	**Treatment**	**Reasoning**
Consumers' Security and Privacy	Mrs. Jackson	Confidentiality	A 12.6.1 - Control of technical vulnerabilities	The novelty of the technology makes undetected vulnerabilities likely and effort should be spent in detecting those.
Consumers' Security and Privacy	Mrs. Jackson	Confidentiality	A 10.10.5 - Fault Logging	The logging of all events regarding the smart meter supports the analysis of what may lead to a data leakage of energy consumption data. The novelty of the technology and lack of experience with attackers in this domain makes it essential to be able to retrace steps of an attacker via logs and to detect the vulnerability that caused this problem.

Continued on next page

Table 18 – continued from previous page

Asset	Asset owner	Security objective	Treatment	Reasoning
Consumers' Security and Privacy	Mrs. Jackson	Confidentiality	A 13.2.3 - Collection of Evidence	An attacker may enter the smart meter without authorization and change the configuration to send energy consumption data every 15 minutes. The energy supplier is violating legal norms like the German BDSG if this happens, because the data are send without an informed consent of the consumer. If a detailed log can prove that the energy supplier was not the one that initiated this configuration the penalty after prosecution is likely to be lower.
Consumers' Energy Consumption Data	Mr. Jones	Confidentiality	A.12.5.4 - Information Leakage Control	The new technology of the smart meters can lead to a loss of the energy consumption data. It should be checked what can be done to prevent information from leaking, either on the design side of the smart meters via separation of data in the devices or ensure that the data can only be read by the energy supplier, e.g., via encryption mechanism.
Consumers' Energy Consumption Data	Mr. Jones	confidentiality	A.11.4.6 - Network Connection Control	Network connection have to be authenticated properly and it also has to be assured that transmissions cannot lead to a leakage of information. For example, even if the data is encrypted, a flaw in the protocol (e.g., that energy consumption data is only send to the energy supplier if energy is actually consumed) might cause information leakage. In this case, missing transmissions between the consumer and the energy supplier could indicate that the consumer is not at home (and not consuming energy), and in turn trigger burglary.
Consumers' Energy Consumption Data	Mr. Jones	Confidentiality	A.11.4.2 - User authentication for external connections	All external users that connect to the smart meter have to be authenticated in order to avoid the unauthorized change of its configuration.

Continued on next page

Table 18 – continued from previous page

Asset	Asset owner	Security objective	Treatment	Reasoning
Consumers' Energy Consumption Data	Mr. Jones	Confidentiality	A.13.2.2 - Learning from information security incidents	The new system depends upon a detailed recording of security events to facilitate later analyses. These can also lead to the discovery of new vulnerabilities.
...	...	...	...	...

We list all the controls that are not selected for an asset in the control exclusion table, which is depicted in Tab. 19. The table lists the asset in the first column, the control in question in the second, and the reason for not selecting the control in the last column. The control overview table and the control exclusion table form the statement of applicability (SOA) for the ISO 27001 documentation. The SOA provides a reasoning of the controls selected for the ISMS.

Table 19. Control exclusion table

Asset	Control	Reason for control exclusion
Home Agent's Configuration	A.11 - Access Control	The distribution and organization of the home agent's are not part of the scope of the ISMS. In addition, the consumer is acquiring and configuring the home agent, and the energy supplier has no influence on the configuration of these devices.
Smart Appliances' Configuration	A.12 - Information systems acquisition, development and maintenance	The consumer is acquiring and maintaining the smart appliances. Hence, the energy supplier has no influence on which smart appliances are part of the smart home. In addition, the energy supplier does not develop or maintain the appliances, and these activities can therefore not be influenced
...	...	...

The control effectiveness measure table shown in Tab. 20 lists all controls and describes how to measure them. The ISMS Procedure and Control Table is depicted in Tab. 21. The table lists the procedures and the controls necessary to ensure the protection of each asset. The table states the asset in the first column, the treatment or control in the second table, the target description in the third, and a description of how the procedure or control is applied in the last column.

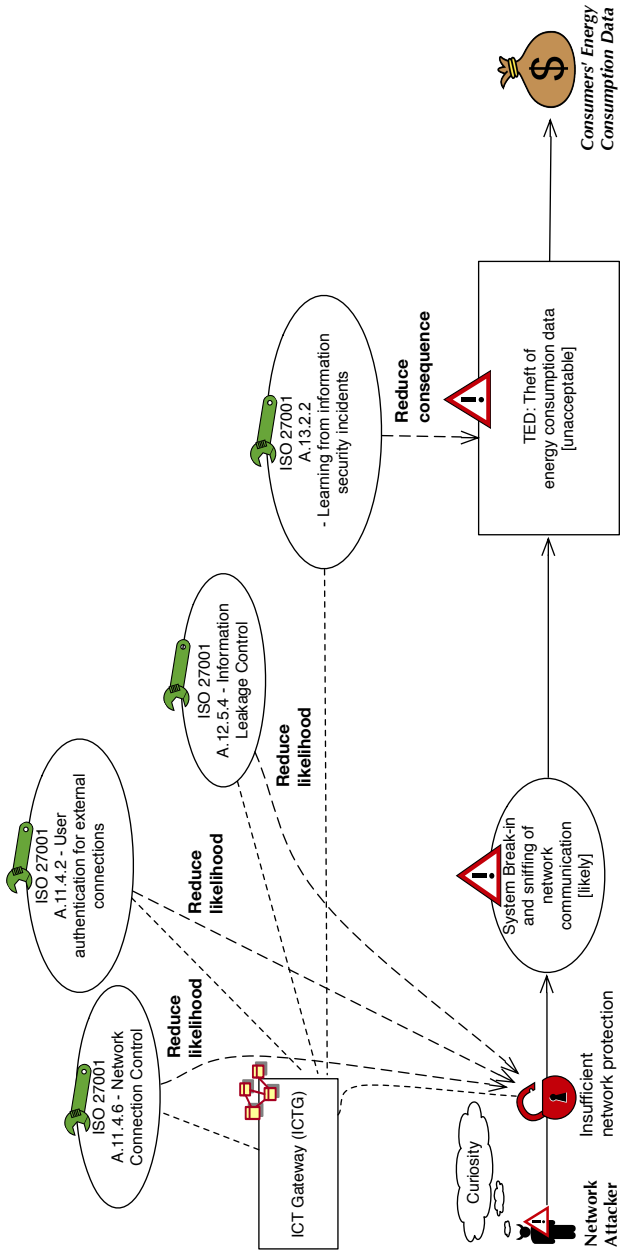

Fig. 18. Treatment Diagram II

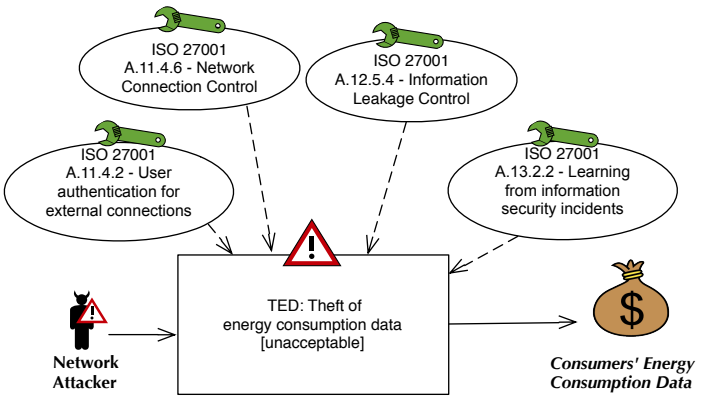

Fig. 19. Treatment Overview Diagram II

Table 20. Control Effectiveness Measure Table

Treatment	**Effectiveness Measure**
A 12.6.1 - Control of technical vulnerabilities	Check if new vulnerabilities are found Check if found vulnerabilities are fixed
A 13.1.2 - Reporting security weakness	Check if weaknesses are reported Conduct interviews and check if weaknesses are known that are not reported
A 10.10.5 - Fault Logging	Check if a logging system is working properly via e.g. functional testing
...	...

Table 21. ISMS Procedure and Control Table

Asset	Treatment	Target Element(s)	Procedure or Control
Consumers' Security and Privacy	A 12.6.1 - Control of technical vulnerabilities	Smart Meter (SM)	Technical vulnerabilities have to be identified, e.g., via penetration testing. These vulnerabilities have to be patched. We define a security black box penetration testing once a month for the first twelve month the device is operational and afterwards every two months.
Consumers' Security and Privacy	A 10.10.5 - Fault Logging	Smart Meter (SM)	In case the smart meter has a malfunction or is attacked, it is important to document the event to prevent future occurrences. A check has to verify that the logging functionality is activated and that the information in the log is sufficient to trace unwanted events. These checks should be conducted once a month.
Consumers' Security and Privacy	A 13.2.3 - Collection of Evidence	Smart Meter (SM)	The collection of evidence regarding unwanted events is important for a new technology like smart meters. This can happen via logging (see also Control A 10.10.5 - Fault Logging) or via external observation of the smart using, e.g., network monitoring tools that check the traffic to and from the device. The chosen mechanisms should be checked once every two month to ensure their viability.
Consumers' Energy Consumption Data	A.12.5.4 - Information Leakage Control	Smart Meter (SM)	The SM shall be configured in such a way that network connections from any device in the smart home have to be initiated from the CHED if the SM shall respond with energy consumption data. The settings have to be tested every six month.
Consumers' Energy Consumption Data	A.11.4.6 - Network Connection Control	ICT Gateway (ICTG)	The ICTG has to control that only devices from inside the smart home can connect to the SM. The configuration of the ICTG has to be checked every six month.
Consumers' Energy Consumption Data	A.11.4.2 - User authentication for external connections	Smart Meter (SM)	If external parties connect to the SM the connection has to be routed via the SSN. All users that access the SM have to be authenticated. This setting of the SM has to be checked every six month.
Consumers' Energy Consumption Data	A.13.2.2 - Learning from information security incidents	Smart Meter (SM)	When the logs or other sources report on security incidents involving the SM, these incidents shall be analyzed. Every six months this information of SM has to be checked and a meeting has to take place that documents these events and the actions that must be taken by the energy supplier to prevent further occurrences.
...	...	...	...

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 [27] 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 [28]. 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 [29] 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 [30] 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 [31], 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 [32] and Kersten et al. [33] provide advice for an ISO 27001 realization. In addition, Klipper [34] 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, 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 [35] 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 [36]. However, the authors do not present a holistic method to information security.

Works also exist that aim at improving the establishment of an ISMS via automation. Mondetino et al. investigate possible automation of controls that are listed in the ISO 27001 and ISO 27002 [37]. 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 [8] there exists a security requirements engineering approach that uses the standard as a baseline for a method. Mellado et al. [38] 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 [39]. 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 [40] 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 report 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.

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. Lund, M.S., Solhaug, B., Stølen, K.: Model-Driven Risk Analysis: The CORAS Approach. Springer (2011)
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: Proceedings of the International Symposium on Engineering Secure Software and Systems (ESSoS). LNCS, Springer (2012) 14–21
4. ISO/IEC: Risk management — Principles and guidelines. ISO/IEC 31000, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2009)
5. ISO/IEC: Information technology - security techniques - information security risk management. ISO/IEC 27005, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2008)
6. Beckers, K., Faßbender, S., Küster, J.C., Schmidt, H.: A pattern-based method for identifying and analyzing laws. In: Proceedings of the International Working Conference onRequirements Engineering: Foundation for Software Quality (REFSQ). LNCS, Springer (2012) 256–262
7. Faßbender, S., Heisel, M.: From problems to laws in requirements engineering using model-transformation. In: ICSOFT 2013 - Proceedings of the 8th International Conference on Software Paradigm Trends, INSTICC, SciTePress (2013) 447–458
8. ISO/IEC: Common Criteria for Information Technology Security Evaluation. ISO/IEC 15408, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2009)
9. Tran, L.M.S., Solhaug, B., Stølen, K.: An approach to select cost-effective risk countermeasures. In: In Proc. 27th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec'13). LNCS 7964, Springer (2013) 266–273
10. Aloula, F., Al-Alia, A.R., Al-Dalkya, R., Al-Mardinia, M., El-Hajj, W.: Smart Grid Security: Threats, Vulnerabilities and Solutions. Intelnational Journal of Smart Grid and Clean Energy **1**(1) (2012) 1–6
11. Lin, H., Fang, Y.: Privacy-aware profiling and statistical data extraction for smart sustainable energy systems. Smart Grid, IEEE Transactions on **4**(1) (2013) 332–340
12. UML Revision Task Force: OMG Unified Modeling Language (UML), Superstructure. http://www.omg.org/spec/UML/2.3/Superstructure/PDF.
13. 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 '13, ACM (2013) 1173–1182
14. Kreutzmann, H., Vollmer, S., Tekampe, N., Abromeit, A.: Protection profile for the gateway of a smart metering system. Technical report, BSI (2011)
15. Soriano, R.: Evaluation of general requirements according state of the art. Technical report, OPEN node project (2010)
16. QUERIC, A.: Functional Use cases. Technical report, OPEN node project (2011)
17. Romero, G., Tarruell, F., Mauri, G., Pajot, A., Alberdi, G., Arzberger, M., Denda, R., Giubbini, P., Rodríguez, C., Miranda, E., Galeote, I., Morgaz, M., Larumbe, I., Navarro, E., Lassche, R., Haas, J., Steen, A., Cornelissen, P., Radtke, G., Kneitinger, H.W., Wiedemann, T., Martínez, C., Ángel Orcajada: Report on the identification and specification of functional, technical, economical and general requirements of advanced multi-metering infrastructure, including security requirements. Technical report, OPEN meter project (2009)

18. 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). (2001) 4–5
19. Opdahl, A.L., Sindre, G.: Experimental comparison of attack trees and misuse cases for security threat identification. Inf. Softw. Technol. **51** (2009) 916–932
20. 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), IEEE Computer Society (2013) 111–120
21. Beckers, K., Côté, I., Hatebur, D., Faßbender, S., Heisel, M.: Common Criteria CompliAnt Software Development (CC-CASD). In: Proceedings 28th Symposium on Applied Computing, ACM (2013) 937–943
22. Swiderski, F., Snyder, W.: Threat Modeling. Microsoft Press (2004)
23. Howard, M., LeBlanc, D.: Writing Secure Code. 2nd edn. Microsoft Press (2003)
24. Knyrim, R., Trieb, G.: Smart metering under eu data protection law. International Data Privacy Law **1** (2011) 121 – 128
25. Raabe, O., Lorenz, M., Pallas, F., Weis, E.: Datenschutz im smart grid und in der elektromobilität. Technical report, KIT (2011) `http://compliance.zar.kit.edu/21_438.php`.
26. Karg, M.: Datenschutzrechtliche Bewertung des Einsatzes von intelligenten Messeinrichtungen für die Messung von gelieferter Energie (Smart Meter). Technical report, ULD (2009) `https://www.datenschutzzentrum.de/smartmeter/20090925-smartmeter.html`.
27. Alberts, C.J., Dorofee, A.J.: OCTAVE Criteria. Technical Report CMU/SEI-2001-TR-016, CERT (December 2001)
28. Siemens: CRAMM – The total information security toolkit. `http://www.cramm.com/` [accessed: January 15, 2013]
29. Agence nationale de la sécurité des systèmes d'information: EBIOS 2010 – Expression of Needs and Identification of Security Objectives. (2010) In French.
30. Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence: The Security Risk Management Guide. (2006)
31. Peltier, T.R.: Information Security Risk Analysis. 3rd edn. Auerbach Publications (2010)
32. Calder, A.: Implementing Information Security based on ISO 27001/ISO 27002: A Management Guide. Haren Van Publishing (2009)
33. Kersten, H., Reuter, J., Schröder, K.W.: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Vieweg+Teubner (2011)
34. Klipper, S.: Information Security Risk Management mit ISO/IEC 27005: Risikomanagement mit ISO/IEC 27001, 27005 und 31010. Vieweg+Teubner (2010)
35. Cheremushkin, D.V., Lyubimov, A.V.: An application of integral engineering technique to information security standards analysis and refinement. In: Proceedings of the international conference on Security of information and networks. SIN '10, ACM (2010) 12–18
36. Lyubimov, A., Cheremushkin, D., Andreeva, N., Shustikov, S.: Information security integral engineering technique and its application in isms design. In: Proceedings of the International Conference on Availability, Reliability and Security (ARES), IEEE Computer Society (2011) 585–590
37. Montesino, R., Fenz, S.: Information security automation: how far can we go? In: Proceedings of the International Conference on Availability, Reliability and Security (ARES), IEEE Computer Society (2011) 280–285
38. Mellado, D., Fernandez-Medina, E., Piattini, M.: A comparison of the common criteria with proposals of information systems security requirements. In: Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on. (april 2006) 8 pp.

39. Mellado, D., Fernández-Medina, E., Piattini, M.: Applying a security requirements engineering process. In Gollmann, D., Meier, J., Sabelfeld, A., eds.: Computer Security – ESORICS 2006. Volume 4189 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg (2006) 192–206
40. Ardi, S., Shahmehri, N.: Introducing vulnerability awareness to common criteria's security targets. In: Software Engineering Advances, 2009. ICSEA '09. Fourth International Conference on. (sept. 2009) 419 –424
41. ISO/IEC: Information technology - Security techniques - Code of practice for information security management. ISO/IEC 27002, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2005)

Appendix

A Comparing ISO 27001 and ISO 31000

Although the ISO 27001 standard and the CORAS approach are the most important references for ISMS-CORAS, we have also based the approach on ISO 31000. Due to some differences between the three, we make a comparison between them in this appendix. We show the differences of several terms of risk management in these two standards, and how these are defined in CORAS. Afterwards, we compare relevant terms and sections of the standards. The aim of our work is to create a method that supports the ISO 27001 standard. Hence, our aim is to identify which sections in ISO 31000 are similar to ISO 27001 sections, and which ISO 27001 sections that do not have equivalents in ISO 31000.

A.1 Terminology Comparison: Risk Assessment

In ISO 31000 [4, Sect. 2.1] risk is defined as the effect of uncertainty on objectives. This is a quite general definition, but five notes are added to elaborate on the term. 1) An effect is a deviation from the expected — positive and/or negative. 2) Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). 3) Risk is often characterized by reference to potential events and consequences, or a combination of these. 4) Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence. 5) Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood. The CORAS approach is mainly based on the definition of the fourth note, i.e. the likelihood of an unwanted incident (an event) and its consequence for a specific asset. ISO 27001 does not give an explicit definition of the term risk in isolation; the standard only contains definitions of related terms, such as risk treatment and risk acceptance. Notice, however, that its terminology refers heavily to ISO/IEC Guide 73 where risk is defined as in ISO 31000.

We will discuss the similarities and differences of further relevant terms in the following.

Fig. 20 gives an overview of the terms that are used to define the risk assessment process in ISO 27001 and CORAS. In ISO 27001 *risk assessment* includes *risk analysis* and *risk evaluation*, and risk analysis in turn includes *risk identification* and *risk estimation*.

CORAS is based on the ISO 31000, both of which use slightly different definitions of the terms risk analysis and risk assessment. ISO 31000 defines risk assessment as the “overall process of risk identification, risk analysis and risk evaluation ”[4, p. 4]. Risk analysis is a “process to comprehend the nature of risk and to determine the level of risk ”. Two notes further elaborates on the term by stating that risk analysis provides the basis for risk evaluation and decisions about risk treatment, and that risk analysis includes risk estimation [4, p. 5]. ISO 31000 further states that the risk levels are derived from the likelihoods and consequences.

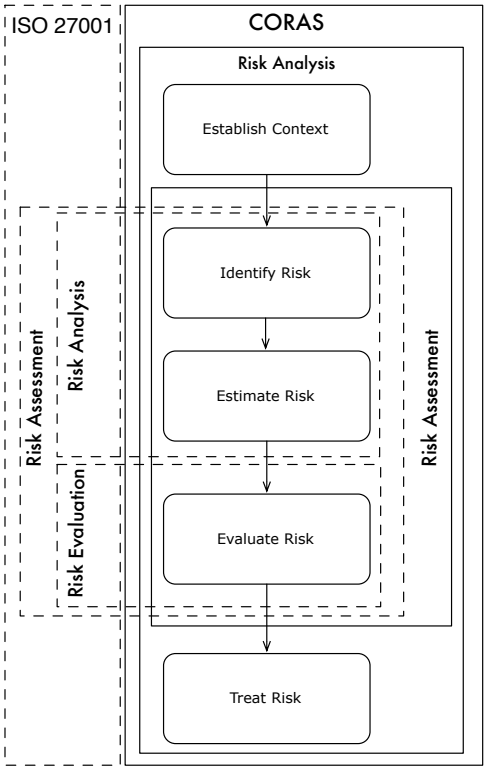

Fig. 20. Risk Terms in CORAS and ISO 27001

The term risk analysis is defined differently in CORAS, where it is defined as a process that includes phases to *establish context*, *identify risk*, *estimate risk*, *evaluate risk*, and *treat risk*. Whereas the term *risk assessment* includes *risk analysis* in the ISO 27001 standard, this is not the case in CORAS. However, on both accounts *risk assessment* involves the activities *identify risk*, *estimate risk*, and *evaluate risk*,

To sum up CORAS, ISO 27001, and ISO 31000 all define risk assessment to include risk identification, risk estimation, and risk evaluation. However, the definition of risk analysis differs in all three. In the following we use the terminology according to the definitions in CORAS, but we state explicitly the mapping to the ISO 27001 terminology.

ISMS-CORAS is an approach to conduct and document a security risk assessment, and this activity as demanded by ISO 27001 risk assessment can be achieved by the CORAS steps risk identification, risk estimation and risk evaluation. In addition, the context establishment part of the CORAS process must be included since these produce essential inputs for the subsequent risk assessment. The Legal CORAS extension sat-

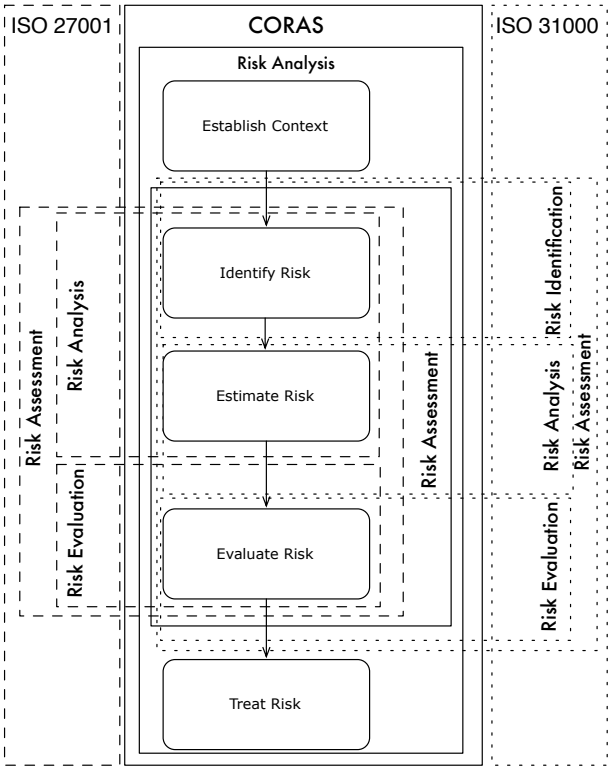

Fig. 21. Risk Terms in CORAS, ISO 27001 and ISO 31000

isfies also the condition that the risk assessment methodology shall be able to consider legal and regulatory requirements (see ISO 27001 Sect. 4.2.1 c 1)).

A.2 General Term Comparison

In order to elicit the requirements that CORAS has to fulfill in order to support the ISO 27001 standard, we have to analyze the differences between the ISO 31000 standard (which CORAS already supports) and the ISO 27001 standard. In Tab. 22, Tab. 23 and Tab. 23 we show the document outlines of the standards, where the former is structured according to the defined terms. We focus on the terms of ISO 27001 and not ISO 31000, because our aim is to support the former. The following terms are defined in ISO 27001 only:

- asset
- availability
- confidentiality

- information security
- information security event
- information security incident
- information security management system ISMS
- integrity
- statement of applicability

A.3 Section Comparison

The ISO 27001 standard describes the requirements for an Information Security Management System (ISMS). The subsections of *Section 4.2.1 Establishing and managing the ISMS* describe the required steps to built an ISMS. *Sect. 4.2.1 a* requires a context and scope description of the ISMS. In the ISO 31000 standard *Sect. 4.3.1* demands also an description of the organization and its context, and ISO 31000 *Sect. 5.3.* demands a description of the risk management context.

Table 22. ISO 27001 and ISO 31000 comparison of the chapters (1/3)

ISO 27001	***ISO 31000***
3. Terms and definitions	***2. Terms and definitions***
asset	risk
availability	risk management
confidentiality	risk management framework
information security	risk management policy
information security event	risk attitude
information security incident	risk management plan
information security management system ISMS	risk owner
integrity	risk management process
residual risk	establishing the context
risk acceptance	external context
risk analysis	internal context
risk assessment	communication and consultation
risk evaluation	stakeholder
risk management	risk assessment
risk treatment	risk identification
statement of applicability	risk source
	event
	consequence
	likelihood
	risk profile
	risk analysis
	risk criteria
	level of risk
	risk evaluation
	risk treatment
	control
	residual risk
	monitoring
	review

Table 23. ISO 27001 and ISO 31000 comparison (2/3)

ISO 27001	***ISO 31000***
4. Information security management system	***4. Framework***
4.1 General requirements	4.1 General
4.2 Establishing and managing the ISMS	4.2 Mandate and commitment
4.2.1 Establishing and managing the ISMS	4.3 Design of framework for managing risk
4.2.1 a Define scope and boundaries	4.3.1 Understanding of the organization and its
4.2.1 b Define ISMS policy	context
4.2.1 c Define risk assessment	4.3.2 Establishing risk management policy
4.2.1 d Identify the risk	4.3.3 Accountability
4.2.1 e Analyse and evaluate risk	4.3.4 Integration into organizational processes
4.2.1 f Identify risk treatment	4.3.5 Resources
4.2.1 g Select controls	4.3.6 Establishing internal communication and
4.2.1 h,i Obtain management approval	reporting mechanisms
4.2.1 j Prepare a statement of applicability	4.3.7 Establishing external communication
4.2.2 Implement and operate the ISMS	and reporting mechanisms
4.2.3 Monitor and review the ISMS	4.4 Implementing risk management
4.2.4 Maintain and improve the ISMS	4.4.1 Implementing the framework for manag-
4.3 Documentation requirements	ing risk
4.3.1 General	4.4.2 Implementing the risk management pro-
4.3.2 Control of documents	cess
4.3.3 Control of records	4.5 Monitoring and review of the framework
	4.6 Continual improvement of the framework

ISO 27001 *Sect. 4.2.1 b* requires a definition of an *ISMS policy*. ISO 31000 requires a *risk management policy*. An ISMS policy [1, Sect. 4.2.1]:“

1. includes a framework for setting objectives and establishes an overall sense of direction and principles for action with regard to information security;
2. takes into account business and legal or regulatory requirements, and contractual security obligations;
3. aligns with the organization’s strategic risk management context in which the establishment and maintenance of the ISMS will take place;
4. establishes criteria against which risk will be evaluated (see 4.2.1c)); and
5. has been approved by management.”

ISO 31000 does not demand an ISMS policy, but a risk management policy instead. A risk management policy according to ISO 31000 is “statement of the overall intentions and direction of an organization related to risk management”[4, Sect. 2.4]. Risk management is “coordinated activities to direct and control an organization with regard to risk”[4, Sect. 2.2].

Hence, both standards demand policy statements concerning risk. However, the ISMS policy demands further directions for information security that also consider business and legal regulations. In order to extend CORAS to support ISMS policy design, we have extend the approach for these tasks. CORAS has already extensions for legal regulations [2], thus the focus of the extension is on information security.

The following demands exist in both standards:

Table 24. ISO 27001 and ISO 31000 comparison (3/3)

ISO 27001	***ISO 31000***
5. Management responsibility	***5. Process***
5.1 Management commitment	5.1 General
5.2 Resource management	5.2 Communication and consultation
	5.3 Establishing the context
	5.3.1 General
	5.3.2 Establishing the external context
	5.3.3 Establishing the internal context
	5.3.4 Establishing the context of the risk management process
	5.3.5 Defining risk criteria
	5.4 Risk assessment
	5.4.1 General
	5.4.2 Risk identification
	5.4.3 Risk analysis
	5.4.4 Risk evaluation
	5.5 Risk treatment
	5.5.1 General
	5.5.2 Selection of risk treatment options
	5.5.3 Preparing and implementing risk treatment plans
	5.6 Monitoring and review
	5.7 Recording the risk management process

- ISO 27001 *Sect. 4.2.1 c* requires a risk assessment, this is also requires for ISO 31000 Sect.*5.4*.
- ISO 27001 *Sect. 4.2.1 d* requires risk identification, which is also demand in ISO 31000 *Sect. 5.4.2*.
- ISO 27001 *Sect. 4.2.1 e* requires risk analysis and evaluation, which is demanded in ISO 31000 *Sect. 5.4.3* and *5.4.4*.
- ISO 27001 *Sect. 4.2.1 f* requires risk treatment identification, which is demanded in ISO 31000 *Sect. 5.5*.
- ISO 27001 *Sect. 4.2.1 h,i* demands management approval, which is similar to ISO 31000 *Sect. 4.2*.

ISO 27001 *Sect. 4.2.1 j* demands a statement of applicability. A statement of applicability is a [1, Sect. 3.16] "documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS. NOTE: Control objectives and controls are based on the results and conclusions of the risk assessment and risk treatment processes, legal or regulatory requirements, contractual obligations and the organization's business requirements for information security". This is similar to ISO 31000 *Sect. 5.5.2 Preparing and implementing risk treatment plans*.

ISO 27001 *Sect. 4.2.1 g* demands to select controls, which is similar to ISO 31000 *Sect. 5.5*. The term control is defined in the standard ISO 27002, which refines the ISO 27001. According to ISO 27002 [41, Sect. 2.2] a Control is a "means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature. NOTE Control is also used as a synonym for safeguard or countermeasure".

The ISO 31000 [4, Sect. 2.26]defines a control as a "measure that is modifying risk (2.1). NOTE 1 Controls include any process, policy, device, practice, or other actions

which modify risk. NOTE 2 Controls may not always exert the intended or assumed modifying effect.".

In both standards controls modify risks and can include policies, procedures, guidelines, practices. In the ISO 27001 a control can also explicitly be a organizational measure, e.g., an administrative or legal action. These are also implicitly in the ISO 31000 definition, because the can be measures that modify risk.

Technology for a better society

www.sintef.no