A Structured Comparison of Security Standards*

Kristian Beckers[1], Isabelle Côté[3], Stefan Fenz[2],
Denis Hatebur[1,3], and Maritta Heisel[1]

[1] paluno - The Ruhr Institute for Software Technology -
University of Duisburg-Essen, Germany
{firstname.lastname}@paluno.uni-due.de
[2] Vienna University of Technology, Austria
{stefan.fenz}@tuwien.ac.at
[3] ITESYS
Dortmund, Germany
{i.cote,d.hatebur}@itesys.de

Abstract. A number of different security standards exist and it is difficult to choose the right one for a particular project or to evaluate if the right standard was chosen for a certification. These standards are often long and complex texts, whose reading and understanding takes up a lot of time. We provide a conceptual model for security standards that relies upon existing research and contains concepts and phases of security standards. In addition, we developed a template based upon this model, which can be instantiated for given security standard. These instantiated templates can be compared and help software and security engineers to understand the differences of security standards. In particular, the instantiated templates explain which information and what level of detail a system document according to a certain security standard contains. We applied our method to the well known international security standards ISO 27001 and Common Criteria, and the German IT-Grundschutz standards, as well.

Key words: structured comparison; security standards, conceptual model, template

1 Introduction

IT systems become increasingly complex considering the amount of stakeholders and technical parts involved. This complexity makes it hard for customers to trust IT systems. In order to gain their customers' trust, companies have to achieve an acceptable security level. Security standards, e.g. the ISO 27000 series

*This research was partially supported by the EU project Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS, ICT-2009.1.4 Trustworthy ICT, Grant No. 256980) and the Ministry of Innovation, Science, Research and Technology of the German State of North Rhine-Westphalia and EFRE (Grant No. 300266902 and Grant No. 300267002).

of standards [1] or the Common Criteria (CC) [2], offer a way to achieve this goal. Security standard implementation concerns the development of secure systems, processes, and documents. Implementing security standards is difficult, due to the limited support for system development and documentation provided in the standards.

Security concerns protecting a system against an attacker, who exploits vulnerabilities in the system to harm assets of stakeholders. Security vulnerabilities in software can be treated with countermeasures against threats. However, eliminating all vulnerabilities is difficult, due to monetary and time constraints. Risk management in the context of security concerns the reduction of the probability of a threat and the limitation of its consequences. Thus, the remaining risk can be used as a criteria for countermeasures for vulnerabilities. In addition, the risk of an entire system has to be calculated using risk management. Risk management is a part of security standards, but specific risk management standards exist, e.g. ISO 31000 [3], which consider the topic in more detail. Hence, we investigate risk management as considered in security standards in this work.

We contribute a conceptual model of security standards, based on existing research such as the works of Sunyaev [4] and the experience of the authors. Moreover, we use this model to investigate methodologies for security and risk management in order to understand their similarities and differences. We developed a template that is based on this model. In particular, fields in the template correspond to the concepts in the model. The template can be instantiated for different security standards. Hence, the instantiated templates can be used to compare different security standards by comparing the instantiated fields, e.g., which kind of environment description the different standards demand. The instantiated templates provide a process independent high level overview of the complete security standards, which helps to learn about standards, what to expect from a system documentation according to a specific standard, and select an appropriate standard for certification. We provide tool support for collecting, storing, and comparing the information collected using our template. Our tool support offers the functionality to compare instantiated templates by displaying their attributes next to each other. The results of this comparison can support the selection of a security standard or an evaluation if further standards should be considered. Moreover, the instantiated template can also provide a simple overview of different standards in order to gain an understanding of relevant concepts of a standard with little effort. Moreover, an understanding of the prescribed process of the standards and its documentation demands helps to judge an existing certification of an IT system. Our template provides an overview of the security analysis demanded by the standards and one can decide if this analysis is sufficient enough in order to trust the certification of a system. We applied our method to the international security standards ISO 27001 [1] and Common Criteria [2]. These standards were chosen because of their wide spread application in the industry[4,5,6]. In addition, we added the German IT-Grundschutz standards [5] as an example for a national security standard.

2 A Method for Comparing Security Standards

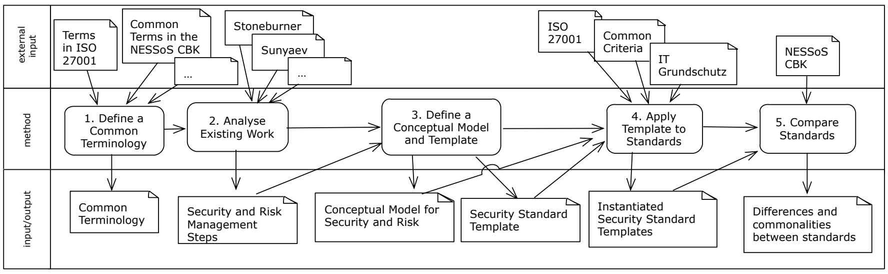

external input
method
input/output
Terms in ISO 27001
Common Terms in the NESSoS CBK
...
Stoneburner
Sunyaev
...
ISO 27001
Common Criteria
IT Grundschutz
NESSoS CBK
1. Define a Common Terminology
2. Analyse Existing Work
3. Define a Conceptual Model and Template
4. Apply Template to Standards
5. Compare Standards
Common Terminology
Security and Risk Management Steps
Conceptual Model for Security and Risk
Security Standard Template
Instantiated Security Standard Templates
Differences and commonalities between standards

Fig. 1. A Method for CompAring SecuriTy standards (CAST)

In the following, we present the steps of our method for CompAring SecuriTy standards (CAST) (see Fig. 1).

1. **Define a Common Terminology** The Jason institute evaluated the research field of security [6] and concluded that the field is missing a common terminology and a basic set of well defined concepts. We address this concern by defining a common terminology against which the terms of the standards are evaluated. We use the terminology of the ISO 27001 standard and the terms defined in the common body of knowledge (CBK)[7] of the EU project *Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS)*[8] as a basis.
2. **Analyze Existing Work** We aim to base our work on existing research and analyze approaches that provide meta-models for security and risk standards. In particular, we focus on the works of Sunyaev [4], who created a security analysis method by identifying common activities in several security standards and the work of Stoneburner et al.[7], who created a model for risk management as part of the NIST SP 800-30 standard. This analysis results in a set of activities, which are often prescribed in security standards.

[4] ISO statistic: `http://www.iso.org/iso/iso_survey_executive-summary.pdf`

[5] Common Criteria statistic: `http://www.commoncriteriaportal.org/products/stats/`

[6] ISO statistics about ISO 27001 certifications: `http://www.iso.org/iso/database_iso_27001_iso_survey.xls`

[7] `http://www.nessos-cbk.org`

[8] `http://www.nessos-project.eu/`

3. **Define a Conceptual Model and Template** We use the information from the existing work to create a novel conceptual model, which considers the steps identified by Sunyaev and Stoneburner et al. We propose a novel model based on these related works. Hence, our conceptual model considers the phases of security standards and also considers risk management activities explicitly. In order to apply the conceptual model to security standards, we transform it into a template that can be instantiated. The template contains all phases of security standards considered in the conceptual model, as well as a description on *how* these phases have to be instantiated for a particular standard.
4. **Apply Template to Standards** In this phase, we instantiate the template for well-known security standards such as Common Criteria [2] , ISO 27001 [1], and the IT Grundschutz standards [5].
5. **Compare Standards** We compare the standards via comparing the different instantiations of our templates. In addition, we consider which of our common terms are considered by the standards and which are not. These insights shall provide a basis for the evaluation of a particular standard.

3 CAST Step 1: Define a Common Terminology

We propose a common terminology for security standards and define terms based on different sources. The purpose of the common terminology is to provide fixed definitions of important terms with regard to security standards as a baseline to which the terms in the individual standards can be compared. Using this comparison, it can be analyzed, which terms are used in the standards for the terms with the meaning defined below. We selected relevant terms for security standards in the terminology based on the experience of the authors and their industry contacts. In addition, we used definitions of these terms from well-known sources. In the following, we list the terms related to security defined in the ISO 27001 standard [1].

Asset anything that has value to the organization

Availability the property of being accessible and usable upon demand by an authorized entity

Confidentiality the property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Security Control a control shall reduce the risk of an information security incident occurring. Note that we refer to controls also as security control for the remainder of the paper. Note that the ISO 27001 uses just control, but we use security control instead to make it explicit that the control addresses a security concern.

Information Security Incident a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

Integrity the property of safeguarding the accuracy and completeness of assets

We also include the following terms from the NESSoS Common Body of Knowledge (CBK)'s common terminology [8]. These definitions are based on the work of Fabian et al [9].

Stakeholder A stakeholder is an individual, a group, or an organization that has an interest in the system under construction. A stakeholder view describes the requirements of a particular stakeholder. The stakeholders may express different types of requirements.

Vulnerability Stakeholders require a security property to hold for a resource, whose violation implies a potential loss to the stakeholder. This violation can be caused by a vulnerability.

Threat A vulnerability could potentially be exploited by a threat. A realized threat is an attack that actually exploits a vulnerability and is initiated by an attacker.

Attacker An attack actually exploits a vulnerability, and the person initiating the attack is an attacker.

Security Goal A stakeholder's security goal expresses his or her security concerns towards an asset. Security goals are traditionally classified into integrity, confidentiality, and availability goals.

Security requirements Security requirements capture security goals in more detail. A security requirement refines one or more security goals. It refers to a particular piece of information or service that explicates the meaning of the asset it concretizes in the context of the system under construction.

We also include the following terms to determine the focus of security standards.

Machine Jackson [10] defines that the machine is the system or software to be developed. In our context the machine is the thing in the focus of the security analysis process described in security standards.

Environment The environment includes a description of all relevant entities in the environment of the machine and, in particular, the interfaces to these entities to the machine.

Policy Security requirements influence formulating security policies, which contain more information than security requirements. "Security policies state what should be protected, but may also indicate how this should be done." [11, p. 5]. "A security policy is a statement of what is, and what is not, allowed" [12, p. 9] "for us, security boils down to enforcing a policy that describes rules for accessing resources" [13, p. 14] and "security policy is a [...] policy that mandates system-specific [...] criteria for security" [14, p. 34].

Security Functions The machine has descriptions of actual implementable functions that concern the fulfillment of security requirements. The descriptions of these functions are security functions.

4 CAST Step 2: Analyse Existing Work

We base our conceptual model for security standards on the HatSec Method (see Sect. 4.1) and the NIST SP 800-30 standard (see Sect. 4.2),

4.1 The HatSec Method

We base our conceptual model for comparing security standards on the HatSec method, because the author analyzed existing security standards and based his method on the resulting common building blocks of the analyzed standards. Only a few standards in the analysis are specific to the health care domain, but most of them are generic security standards such as ISO 27001 [1]. Moreover, the HatSec method does not create specific building blocks for the medical domain. Hence, the mining of security standard specific building blocks can be re-used for our conceptual model. We rely on the HatSec method as a foundation for our conceptual model, but the difference to our work is that the HatSec method provides a means to conduct a security analysis, while we provide a method to compare the processes, documentation demands, and methodologies in security standards.

The Healthcare Telematics Security (HatSec) method by Sunyaev [4] is a security analysis method developed for the healthcare domain. Sunyaev focuses on security analysis in the investigated standards, even though several of the standards the author investigates concern risk management, as well. However, in these cases the author did not consider the parts in the standards that concern risk in detail. The method consists of seven building blocks, which are derived from the following security and risk management standards: ISO27799 [15] ISO 27001 [1], IT Grundschutz [5], NIST SP 800-30 [7], CRISAM [16], CRAMM [17], ISRAM [18], ISMS JIPDEC for Medical Organisations [19], HB 174-2003 [20], US Department of Health and Human Services - Guideline for Industry, Q9 Quality Risk Management [21]. Note that only the last four standards are specific to the health care domain.

The building blocks of the HatSec method are related to the standard as follows. Each building block of the HatSec method occurs also in these standards. However, not all of the steps in the standards occur in the HatSec method. Fig. 2 shows the seven building blocks of the method. These are further divided into three phases. The *Security Analysis Context and Preparation* phase establishes the context of the security problem. The *Scope Identification* describes the limits of the environment and the system-to-be followed by the *Asset Identification.* The *Security Analysis Process* covers the actual analysis activities of the method. The *Basic Security Check* reveals countermeasures already in place and the *Threat Identification* shows dangers resulting from possible attacks on the system-to-be. The *Vulnerability Identification* reveals vulnerabilities to security properties that are potentially exploited by threats. The original HatSec method demands an iteration between the Basic Security Check and the Threat Identification. However, we propose to rather iterate between the Vulnerability Identification and the Basic Security Check, because countermeasures are in place to mitigate vulnerabilities and only subsequent threats. These two building blocks shall be executed in iterations, e.g., if a threat is detected, it shall be checked if a countermeasure for the vulnerability is already in place. The *Security Assessment* concludes the Security Analysis Process by determining the level of security required and the risks remaining. In addition, the Security Assessment also initiates the *Security Analysis Product* phase, because the *Security Measures* activity evaluates the results of the Security Assessment in order to determine if the chosen level of security is adequate or if changes have to be made, e.g., adding additional security controls.

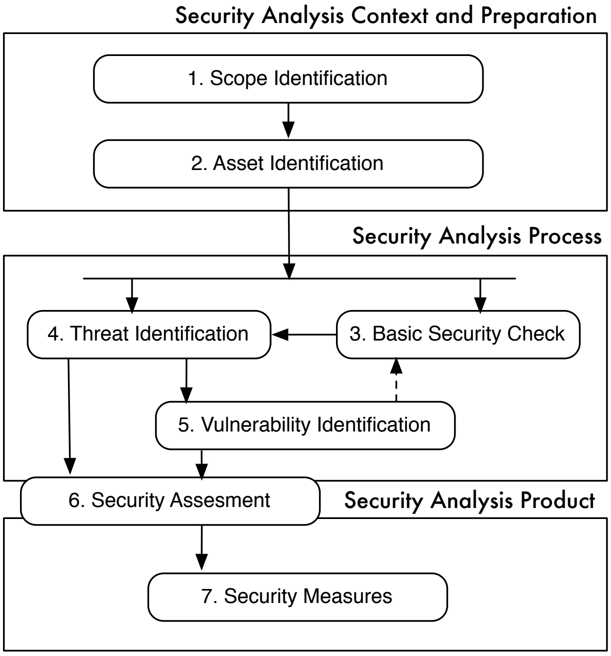


Fig. 2. The HatSec Method by Sunyaev [4]

4.2 NIST SP 800-30 Standard

The entire information security risk management methodology by Stoneburner et al. [7] is subdivided into three main phases: (1) risk assessment, (2) risk mitigation, and (3) evaluation. Risk assessment identifies and evaluates potential risks and their impacts, to recommend preventive and risk-reducing controls. In the risk mitigation phase, the identified risks are prioritized and adequate preventive controls are implemented and maintained. After the control implementation, a continual evaluation phase determines whether the implemented risk-reducing controls decrease the risk to an acceptable level or if further controls are required.

We briefly describe the NIST SP 800-30 risk management methodology, which we use as a basis for adding further building blocks to the HatSec method in order to create a conceptual model to compare security standards and also their approaches towards risk management in more detail. The reasons for having chosen the information security risk management methodology by Stoneburner et al. [7] are: (1) it gives very detailed identification and guidance of what should be considered in the phases of risk assessment, mitigation, and evaluation, (2) the methodology is well-accepted and well-established, (3) it is freely available, and (4) it supports organizations of all sizes. The comparison of the methodology against others shows that the proposed concepts could be easily applied to similar information security risk management methodologies such as ISO 27005 [22] or EBIOS [23] due to the similar structures of these methodologies.

5 CAST Step 3: Define a Conceptual Model

We extended the HatSec Method with several concepts from the NIST SP 800-30 and refined several concepts to ensure a more detailed comparison of security standards. Moreover, we integrated the conceptual model into a sequence of Standard Activities, which are the activities that have to be conducted to establish a security standard. Our conceptual model is shown in Fig. 3, we show example instantiations in Sect. 6. We structure our conceptual model using the three phases *Security Analysis Context and Preparation*, *Security Analysis Process*, and *Security Analysis Product* (see Sect. 4).

We explain the building blocks of the *Security Analysis Context and Preparation* in the following. We split the *scope identification* of the HatSec method into an *environment description* and a *stakeholder description*. The reason is that security is about protection of assets and harm to assets results in a loss to stakeholders. We have to understand the significance of the loss by describing the stakeholder. Moreover, stakeholders can cause threats to assets, and the identification of stakeholders in a scope is a research problem [24,25]. Moreover, we included the building block *Risk Level Description* to include a mechanism to categorize assets already in the beginning of the security analysis. This is done to focus security analysis on assets with a high risk level, as is suggested by NIST SP 800-30 [7] and IT Grundschutz [26].

We describe our building blocks for the *Security Analysis Context and Preparation* phase in the following.

Environment Description The environment description states the scope of the standard. Hence, the environment in which the security system shall be integrated into should be, e.g., an organization or an Information and Communication Technology (ICT)-based System or combinations of both.

Stakeholder Description The stakeholder description describes all relevant persons, organizations, and government bodies that have a relation to the environment.

Asset Identification The asset identification for the stakeholders collects all information or resources that have a value to the stakeholders. The assets shall be protected from harm caused by the environment.

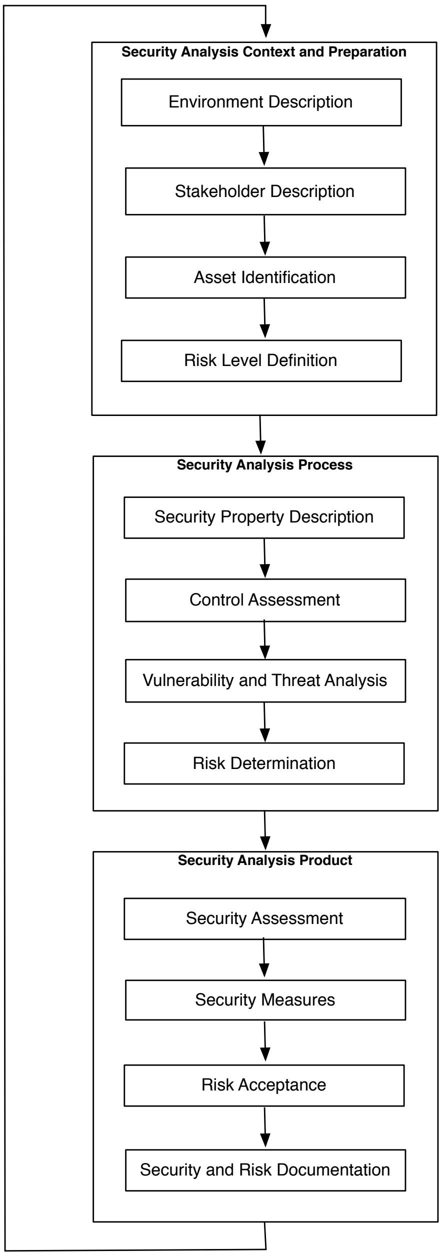

Security Analysis Context and Preparation
Environment Description
Stakeholder Description
Asset Identification
Risk Level Definition
Security Analysis Process
Security Property Description
Control Assessment
Vulnerability and Threat Analysis
Risk Determination
Security Analysis Product
Security Assessment
Security Measures
Risk Acceptance
Security and Risk Documentation

Fig. 3. A Conceptual Framework for Security Standards

Risk Level Description For each asset, a risk level description states the impact the loss of an asset has on a stakeholder. Hence, the risk level description classifies the assets into categories according to their significance for the environment. In this building block the risk level determination is based on the opinion of stakeholders and described on a high level of abstraction.

We explain the building blocks of the *Security Analysis Process* in the following. We divided the building block *Basic Security Check* into a security property definition for assets and an assessment of existing controls. The security properties provide an overview of high level security goals, which should be separated from the *Control Assessment*, since it considers existing security solutions. Moreover, we combined the threat analysis and vulnerability identification, because threats are exploited vulnerabilities [9] and should be considered together in our view. We add also a *Risk Determination* building block to the *Security Analysis Process* that describes how likelihoods and consequences for the resulting threats are assessed.

Security Property Description We initiate the *Security Analysis Process* with a high level security property description, which determines security goals for assets. For example, the ISO 27001 standard uses high level security objectives to "establish an overall sense of direction and principles for action with regard to information security" [1, p. 4] as part of their ISMS policy, the superset of all security policies that the standard establishment creates.

Control Assessment The control assessment determines which controls (either technical ones such as encryption mechanisms or non-technical controls such as security policies) are already in place and their ability to ensure a security property of an assets.

Vulnerability and Threat Analysis The threat analysis assumes vulnerabilities of an asset. Moreover, threats have to be validated by showing that the potentially exploited vulnerability exists. In general, a threat requires a source and an existing vulnerability to become effective. The threat source can either intentionally or accidentally exploit a potential vulnerability. The aim of the threat identification step is to determine potential threats and their corresponding sources such as human threats (e.g. active network attacks, theft, unintentional data alternation, etc.), or environmental threats (e.g. power failure, water leakage, etc.). On the basis of the threat analysis, the vulnerability analysis shows potential vulnerabilities present in the scope, including the consideration of vulnerabilities in the field of (1) management security (e.g. no assignment of responsibilities, no risk assessment, etc.), (2) operational security (e.g. no external data distribution and labeling, no humidity control, etc.), and (3) technical security (e.g. no cryptography solutions in use, no intrusion detection in place, etc.).

Risk Determination The risk determination determines useful likelihood and impact scales to conduct risk management for assets. The risk determination considers the output of all previous steps and evaluates these results with regard to risk, considering the likelihood and impact scales. We explain this step further based on the NIST 800-30 standard in the following.

Probability Level	Probability Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Table 1. NIST 800-30 probability definitions [7]

Firstly, a probability determination is concerned with the probability of a threat exploiting a certain vulnerability in the given system. Therefore, the organization has to deal with the following factors: (1) motivation and capability of the attacker, (2) nature of the vulnerability, and (3) existence and effectiveness of the current controls. Stoneburner et al. [7] propose a qualitative probability rating as stated in Table 1.

Secondly, an impact analysis determines the impact on the organization's ability to perform its mission if a threat should successfully exploit a certain vulnerability. The NIST SP 800-30 information security risk management methodology recommends measuring the impact in terms of the loss of integrity, availability, and/or confidentiality. While some impacts can be measured quantitatively in terms of the revenue lost, NIST recommends the measurement of impacts on a qualitative level (e.g. high, medium, and low). The main problem with quantitative measurement methods is that it is very hard to determine if the impact of a certain threat exactly corresponds to a certain amount of money. How can someone determine that a fire would cause a loss of exactly EUR 923.343 and not EUR 923.443? In most cases, people tend to use quantitative methods in a qualitative way, for example assigning monetary ranges (e.g. EUR 0 - EUR 200.000, EUR 200.000 - EUR 400.000, etc.) to the different impact levels.

Thirdly, the organization now knows the components necessary to determine the actual risk: (1) the probability that a given threat source exploits a certain vulnerability, (2) the impact caused if the threat exploited the very vulnerability, and (3) the adequacy of the existing controls for reducing or eliminating the risk. By multiplying the threat probability with the magnitude of the impact, the organization is able to determine the risk level and thus to plan the necessary actions as stated in Tab. 2.

Finally, we explain the building blocks of the *Security Analysis Product* phase. We use the *Security Assessment* and *Security Measures* building blocks as described in the HatSec method and we add explicit building blocks for *Risk Acceptance* and *Security and Risk Documentation. Risk Acceptance* is an essential step of finishing the security analysis product, and if risks are accepted to soon, the entire security analysis product might not be effective. Hence, we aim to document in the template how the standards address this issue. In addition, the certification process of a security standard is usually based on the documen-

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's administrator must determine whether corrective actions are still required or decide to accept the risk.

Table 2. NIST 800-30 risk scale and necessary actions [7]

tation of the security analysis product. That is why we want to add a description of the demanded documentation in our conceptual model and template.

Security Assessment The security assessment evaluates if the existing security controls satisfy the security properties of the assets considering the results of the *Vulnerability and Threat Analysis*, as well as the *Risk Determination*. This step also describes how further security controls have to be selected. For example, the ISO 27001 standard [1] has a mandatory ANNEX A from which controls have to be selected.

Security Measures The security measures activity specifies a list of new, refined or existing security controls that are required to improve the protection of the assets. This final result of the selection of controls are the *Security Measures*. For example, the ISO 27001 demands a so-called *Statement of Applicability* that reasons about the necessity of the controls in ANNEX A.

Risk Acceptance The risk acceptance evaluates if the *Security Measures* reduce the risk of attacks on assets to acceptable levels. Often a clear cut criteria has to be defined that is fulfilled or not. For example, the controls prevent threats from attackers with a mediocre skills level and a limited amount of time.

Security and Risk Documentation The security system description finishes with the security and risk documentation of the security analysis product. The documentation has to usually follow certain guidelines of a standard.

We mapped our conceptual model to a template presented in Tabs. 14, 15, and 16 in the appendix. We have elicited a series of questions for each building block, which shall help to fill in the required information. In addition, we stated which common terms are relevant for each part of the template.

6 CAST Step 4: Instantiate Template with Standards

We instantiate our template with the ISO 27001 standard (Sect. 6.1), IT Grundschutz (Sect. 6.2), and Common Criteria (Sect. 6.3).

6.1 ISO 27001

The ISO 27001 defines the requirements for establishing and maintaining an Information Security Management System (ISMS) [1]. In particular, the standard describes the process of creating a model of the entire business risks of a given organization and to specify specific requirements for the implementation of security controls. The resulting ISMS provides a customized security level for an organization.

The ISO 27001 standard contains a description of the so-called *ISO 27001 process* [1]. The process contains phases for establishing an ISMS, implementing and operating an ISMS and also monitoring, reviewing, maintaining and improving it.

In the initial phase, the *scope and boundaries* of the ISMS, its *interested parties*, *environment*, *assets*, and all the *technology* involved are defined. In this phase, also the ISMS *policies*, *risk assessments*, *evaluations*, and *controls* are defined. Controls in the ISO 27001 are measures to *modify risk*.

The ISO 27001 standard demands a set of documents that describe the requirements for the ISMS. Furthermore, the standard demands periodic audits towards the effectiveness of an ISMS. These audits are also conducted using documented ISMS requirements. In addition, the ISO 27001 standard demands that management decisions, providing support for establishing and maintaining an ISMS, are also documented. This support has to be documented via management decisions. This has to be proven as part of a detailed documentation of how each decision was reached and how many resources (e.g., personal, budget, time, etc.) are committed to implement this decision. Moreover, certification of an ISMS according to the ISO 27001 standard is possible, based upon the documentation of the ISMS.

Table 3. Instantiation for ISO 27001 of the Security Analysis Context and Preparation Part of the Template for Security Standard Description

Security Analysis Context and Preparation
Environment Description
The machine in this standard is the ISMS and the environment is anything outside the scope of the ISMS. “The standard demands an ISMS scope definition and its boundaries in terms of the characteristics of the business, the organization, its location, assets and technology, and including details of and justification for any exclusions from the scope” [1, p.4,Sect. 4.2.1 a]. The standard mentions the scope explicitly in the following sections. Sect. 4.2.1 d concerns risk identification and the section recommends to consider the scope definition for identifying assets. Section 4.2.3 demands management reviews of the ISMS that also includes to check for possible changes in the scope of the ISMS. Section 4.3 lists the documentation demands of the standard and Sect. 4.3.1 d requires a documentation of the scope of the ISMS. Moreover, the standard demands an explicit to creating an ISMS. In particular, Section 5.1 Management commitment concerns proof the management shall provide for establishing an ISMS objectives, plans, responsibilities and accepting risks. Section 5.2 Resource management concerns the provision of resources for establishing the ISMS and the training of the members of the organization for security awareness and competence.
Stakeholder Description
The stakeholder definition is part of the scope definition. The standard uses the term *Interested Parties* [1, p. vi] instead of stakeholders, who have security “expectations” that are input for the ISMS implementation as well as “security requirements”.
Asset Identification
The design goal of the ISO 27001 ISMS is to protect assets with adequate security controls and this is stated already on page 1 of the standard. This is relevant in particular in Section 4 that describes the ISMS and in particular in Sect. 4.2 - Establishing and managing the ISMS states the scope definition. Section 4.2.1 a demands the definition of assets. Section 4.2.1 b concerns the definition of ISMS security policies demands that the policy shall consider assets. Section 4.2.1 d that concerns risk identification uses the scope definition to identify assets, to analyze threats to assets, and to analyze the impacts of losses to these assets. Section 4.2.1 e concerns risk analysis, which also clearly define to analyze assets and to conduct a vulnerability analysis regarding assets in light of the controls currently implemented.
Risk Level Definition
The standard requires a risk level definition in the steps following the scope definition. Section 4.2.1 b states that the ISMS policy has to align with the risk management. Section 4.2.1 c demands a risk assessment that includes criteria for accepting risks and identify the acceptable risk levels.

Table 4. Instantiation for ISO 27001 of the Security Analysis Process Part of the Template for Security Standard Description

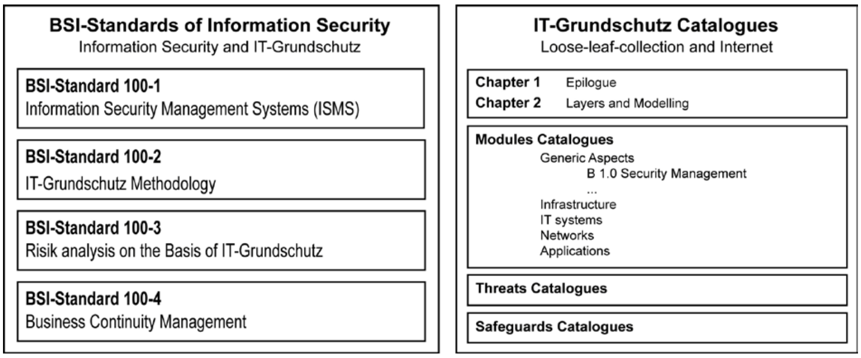
Security Analysis Process
Security Property Description
The standard demands the elicitation of high level security goals in the section after the scope definition, this Section 4.2.1 b concerns the definition of ISMS policies of which high level security goals are a part. “The ISMS policy is considered as a superset of the information security policy.” [1, p. 4].
Control Assessment
The assessment concerns likelihoods of security failures with regard to threats and vulnerabilities. In addition, impacts to assets should be considered of the controls currently implemented according to ISO 27001 Section 4.2.1 e 2.
Vulnerability and Threat Analysis
The ISO 27001 standard concerns threat analysis in several sections for determining the risks to assets. Section 4.2.1 d demands a threat analysis for assets for the purpose of identifying risks and the vulnerabilities that might be exploited by those threats. Section 4.2.1 e concerns risk analysis and evaluation and demands to determine likelihoods and consequences for threats. Section 4.2.4 d concerns the review process of the ISMS and also demands a threat identification. Section 7.2 that concerns the management review of the ISMS also demands a threat analysis.
Risk Determination
The standard demands a description of a methodology for risk management and it mentions several related activities explicitly. Section 4.2.1 d concerns risk identification and Sect. 4.2.1 e demands risk analysis and evaluation.

Table 5. Instantiation for ISO 27001 of the Security Analysis Product Part of the Template for Security Standard Description

Security Analysis Product
Security Assessment
Threats to assets have to be analyzed and existing security controls documented. The risk has to be evaluated of these threats according to the criteria set previously, considering the existing security controls. For all unacceptable risks security controls have to be selected to reduce the risk to acceptable level. The control selection is based on security requirements, which are refinements of the high level security goals. This is explained in the following.
Security Measures
The ISO 27001 standard concerns high level ISMS policies during the establishment of the ISMS to guide the focus of security and security policies as controls that define in detail what a specific security controls should achieve. In particular, the Annex A of the ISO 27001 standard describes the normative controls of the standard. This is stated in Section 4.2.1 f concerning risk treatment and Section 4.2.1 g discussing controls for risk treatment.
Risk Acceptance
Criteria for acceptable have to be defined in the beginning of the risk analysis (Section 4.2.1 c) and after the control selection it has to be shown that the criteria for acceptable risk are fulfilled. The standard also demands management approval for acceptable levels of risk (see Section 4.2.1 h).
Security and Risk Documentation
The ISO 27001 standard demands the following documents: – ISMS policies and objectives – Scope and boundaries of the ISMS – Procedures and controls – The risk assessment methodology – Risk assessment report – Risk treatment plan – Information security procedures – Control and protection of records that can provide evidence of compliance to the requirements of the ISMS – Statement of Applicability describing the control objectives and controls that are relevant and applicable to the organization's ISMS. In addition, the ISO 27001 standard demands the documentation of Management Decisions that provide support for establishing and maintaining an ISMS.

6.2 IT-Grundschutz

The German Bundesamt für Sicherheit in der Informationstechnik (BSI) issued the so-called *BSI series of standards for information security* [26] (see left hand side of Fig. 4). These are based on the ISO 27001 and ISO 27002 standards and refine them with a new methodology. The series of standards consists of BSI-Standard 100-1 that concerns the management issues of the standard such as planning IT processes. The BSI-Standard 100-2 [27] describes the methodology of how to build an ISMS, BSI-Standard 100-3 [5] concerns risk management, and BSI 100-4 [28] considers Business Continuity Management, e.g., data recovery plans. In the following, we focus on BSI 100-2, because it contains the methodology. The BSI standard 100-2 describes how an ISMS can be established and managed. It is compatible to the ISO 27001 standard, meaning that an implementation of the BSI standard 100-2 can be used for an ISO 27001 certification with the German BSI [26, p. 12]. In addition, the standard aims towards reducing the required time for an ISMS implementation. This is achieved by provisioning the IT Grundschutz Catalogues (see right hand side of Fig. 4). This catalog contains a significant collection of IT security threats and controls, and a mapping between them. Note that controls are called *safeguards* in the BSI terminology. The standard offers a method depicted in Fig. 5 that starts with a structural analysis of the organization and the environment. The standard suggests a focus on at least the areas organization, infrastructure, IT-systems, applications, and employees. The next step is to determine the required security level, followed by modeling the security measures, and a basic security check. This security check classifies the assets and executes a risk analysis for the 20 percent of assets with



BSI-Standards of Information Security
Information Security and IT-Grundschutz

BSI-Standard 100-1
Information Security Management Systems (ISMS)

BSI-Standard 100-2
IT-Grundschutz Methodology

BSI-Standard 100-3
Risik analysis on the Basis of IT-Grundschutz

BSI-Standard 100-4
Business Continuity Management

IT-Grundschutz Catalogues
Loose-leaf-collection and Internet

Chapter 1 Epilogue
Chapter 2 Layers and Modelling

Modules Catalogues
Generic Aspects
B 1.0 Security Management
...
Infrastructure
IT systems
Networks
Applications

Threats Catalogues

Safeguards Catalogues

Fig. 4. BSI IT-Grundschutz Overview taken from [26]

the highest security level. The remaining 80 percent are not considered in a risk analysis and simply suggested safeguards in the IT Grundschutz Catalogues for these assets are implemented. After the security check, the measures are consolidated and another basic security check is executed. The last step is realizing the measures.

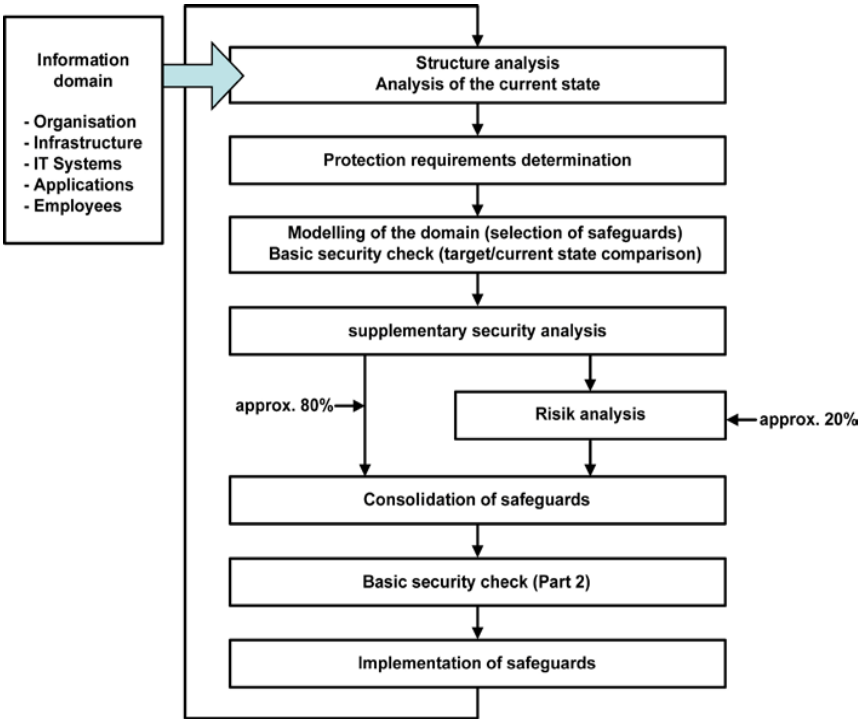

Information domain
- Organisation
- Infrastructure
- IT Systems
- Applications
- Employees
Structure analysis
Analysis of the current state
Protection requirements determination
Modelling of the domain (selection of safeguards)
Basic security check (target/current state comparison)
supplementary security analysis
approx. 80%
Risik analysis
approx. 20%
Consolidation of safeguards
Basic security check (Part 2)
Implementation of safeguards

Fig. 5. IT Grundschutz Method taken from [27]

Table 6. Instantiation for BSI 100.2 of the Security Analysis Context and Preparation Part of the Template for Security Standard Description

Security Analysis Context and Preparation
Environment Description
The standard demands a description of the scope and in particular [27, p. 37]: - "Specify which critical business processes, specialised tasks, or parts of an organisation will be included in the scope - Clearly define the limits of the scope - Describe interfaces to external partners"The machine in this standard is an ISMS and the environment are described via interfaces to external partners. The scope definition is accompanied by a structure analysis, which demands a separate documentation of the following parts of the scope: information, application, IT systems, rooms, communication networks.
Stakeholder Description
The employees of the organization that take part in the business processes have to be documented. Moreover, the users of the scope elements such as applications are documented, as well. These are both part of the scope definition. The standard refers to users or employees of the organization instead of stakeholders.
Asset Identification
For each business process in the scope a level of protection has to be determined. The entire processes and in particular the information technology used and information processed it contains are considered as assets.
Risk Level Definition
The standard uses the protection requirements as an indicator for high level risks.

Table 7. Instantiation for BSI 100.2 of the Security Analysis Process Part of the Template for Security Standard Description

Security Analysis Process
Security Property Description
All general security concerns are specified in an information security policy, which describes the general direction of information security in the organization. In addition, for each asset security goals have to be determined in terms of confidentiality, integrity, and availability. The standard calls them protection requirement, which have to be categorized in the levels: normal, high, and very high [27, p. 48]. These categories have the meaning [27, p. 48]: **Normal** “The impact of any loss or damage is limited and calculable.” **High** “The impact of any loss or damage may be considerable.” **Very High** “The impact of any loss or damage may be of catastrophic proportions which could threaten the very survival of the organisation.” Note that the standard also allows to define a different scale, but this is the scale recommended. The protection requirements are refined with damage scenarios [27, p. 48]: “Violations of laws, regulations, or contracts Impairment of the right to informational self-determination Physical injury Impaired ability to perform the tasks at hand Negative internal or external effects Financial consequences” These damage scenarios have to be put in relation to the protection requirement for each organization that establishes the standard. This means it has to be defined for each category what the damage scenario means, e.g., what means normal financial consequences.
Control Assessment
The standard relies on the security controls listed in the IT Grundschutz catalog. These are categorized into [27, p. 48]: **S 1** Infrastructure, **S 2** Organization, **S 3** Personnel, **S 4** Hardware and software, **S 5** Communication, **S 6** Contingency planning. Several of the threats listed in the IT Grundschutz Catalogues have existing mappings to possibly relevant safeguards. These have to be considered as relevant if a threat is selected. The safeguards have to be refined for the scope. The standard refers to safeguards instead of security controls.
Vulnerability and Threat Analysis
The standard demands a model of the scope. The IT Grundschutz catalog provides modules that support this modeling. These modules are categorized in the following domains [27, p. 48]: *General aspectsInfrastructureIT systemsNetworksApplication*. The modules contain a mapping to the following threat categories: **T 1** Force majeure, **T 2** Organisational shortcomings, **T 3** Human error, **T 4** Technical failure, **T 5** Deliberate acts. All of the threats in each threat category of the IT Grundschutz catalog have to be analyzed with regard to the scope and the relevant threats have to be documented. The threats have to be refined for the scope of the analysis.
Risk Determination
A risk analysis can be conducted either after the basic security check or the supplementary security check. The management has to make a choice, for which assets a risk analysis has to be conducted. The standard does not prescribe a strict methodology for risk management, but provides rather advice for how to consider threats and safeguards and in which step of the method use to apply the threat analysis. It is not providing a method for e.g. eliciting likelihood or consequences scales.

Table 8. Instantiation for BSI 100.2 of the Security Analysis Product Part of the Template for Security Standard Description

Security Analysis Product
Security Assessment
A security assessment is done using a so-called *basic security check*. The model of the scope and the protection requirements are used to develop a security test plan, which determines the effectiveness of existing security controls. Each test has to describe a target state and after conducting the test it is determined if a control is effective by analyzing the state of the tested scope elements. In a sense the security testing plans are based on security requirements, which refine the protection requirements. This basic security check consists of three different steps. “The first step consists of making the organisational preparations and, in particular, selecting the relevant contact people for the target/actual state comparison. In Step 2, the target state is compared to the actual state by conducting interviews and performing random checks. In the final step, the results of the target/actual state comparison are documented together with the reasoning behind the results. ” [27, p. 66].
Security Measures
After considering the threats and safeguards in the IT Grundschutz catalog a supplementary security analysis is conducted. “The supplementary security analysis is to be performed on all target objects in the information domain to which one or more of the following applies: - The target objects have high or very high protection requirements in at least one of the three basic values – confidentiality, integrity, or availability - The target objects could not be adequately depicted (modelled) with the existing modules in the IT-Grundschutz Catalogues - The target objects are used in operating scenarios (e.g. in environments or with applications) that were not foreseen in the scope of IT-Grundschutz. ” [27, p. 66].
Risk Acceptance
Accepted risks have to be documented with a reasoning.
Security and Risk Documentation
Each step of the methodology presented in the standard has to be documented.

6.3 The Common Criteria

The ISO/IEC 15408 - Common Criteria for Information Technology Security Evaluation is a security standard that can achieve comparability between the results of independent security evaluations of IT products. These are so-called *targets of evaluation (TOEs).*

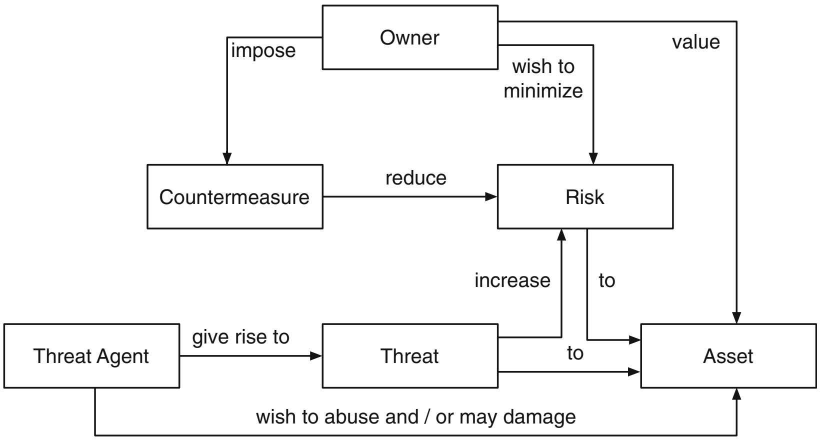


Fig. 6. The Common Criteria Basic Security Model taken from [2]

The Common Criteria (CC) is based upon a general security model (see Fig. 6). The model considers TOE owners that value their assets and wish to minimize risk to these assets via imposing countermeasures. These reduce the risk to assets. Threat agents wish to abuse assets and give rise to threats for assets. The threats increase the risk to assets. The concepts of the Common Criteria consider that potential TOE owners infer their security needs for specific types of TOEs, e.g., a specific firewall. The resulting documents are called Security Targets (ST). Protection profiles (PP) state security needs for an entire class of TOEs, e.g., client VPN application. The evaluators check if a TOE meets its ST. Protection profiles (PP) state the security requirements of TOE owners. TOE developers or vendors publish their security claims in security targets (ST). A CC evaluation determines if the ST is compliant to a specific PP. The standard relies upon documents for certification, which state information about security analysis and taken measures.

Table 9. Instantiation for Common Criteria of the Security Analysis Context and Preparation Part of the Template for Security Standard Description

Security Analysis Context and Preparation
Environment Description
The common criteria demands a description of the TOE in its environment. Hence, the TOE is the machine. The environment contains stakeholders, other software components the TOE requires, e.g., a specific operating system. The standard discusses the environment simply as outside the TOE. "An ST introduction containing three narrative descriptions of the TOE " [2, p. 64, Part 1: Introduction and general model]. The TOE reference provides a description of unique identifications for an ST that describes the TOE such as a version numbers for the revision of the ST. The TOE overview describes the intended functionality of the TOE and security features on a high level of abstraction. The standard describes the TOE and its environment, which is simply referred to as *outside* or *operational environment* of the TOE. Hence, the system consists of the TOE and its *operational environment.*
Stakeholder Description
The Common Criteria focuses on describing a software product and it describes stakeholders just as much as they are required to understand the TOE's functionality or security features. For example, a TOE shall display certain information to a user. The standard uses the term external entity for all stakeholders that interact with the TOE from the outside. It explicitly states that a user is a external entity. Note that the term external entities also includes IT entities [2, p. 16 and p. 20, Part 1: Introduction and general model].
Asset Identification
"Security is concerned with the protection of assets. " [2, p. 38, Part 1: Introduction and general model]. Stakeholders consider assets valuable (see below), which is highly subjective. Thus, the identification of assets depends upon information from stakeholders, because "almost anything can be an asset " [2, p. 38, Part 1: Introduction and general model]. Hence, assets should have a description and also some information regarding the need for protection. This is aligned with descriptions of existing PPs such as [29]. Furthermore, in PPs the concept of a SecondaryAssets is used [29], whose loss do not cause harm to the ToE Owner directly, but the harm can cause harm to an Asset. This in turn can cause a loss to a ToE Owner. The standard defines "assets entities that the owner of the TOE presumably places value upon. " [2, p. 16 and p. 20, Part 1: Introduction and general model].
Risk Level Definition
The Common Criteria concerns risks arising from attacks and the standard does not define basic risk levels, but attack potentials. The scale is basic, enhanced-basic, moderate, high.

Table 10. Instantiation for Common Criteria of the Security Analysis Process Part of the Template for Security Standard Description

Security Analysis Process
Security Property Description
Security needs of assets are expressed in terms of confidentiality, integrity, and availability or other not specified security goals. “Security-specific impairment commonly includes, but is not limited to: loss of asset confidentiality, loss of asset integrity and loss of asset availability.” [2, p. 39]. These terms are not defined in the general term definition section of Part 1, but refined terms are defined in Part 2: security functional components. For example, *FDP_UCT* describes the meaning of user data confidentiality.
Control Assessment
“Subsequently countermeasures are imposed to reduce the risks to assets. These countermeasures may consist of IT countermeasures (such as firewalls and smart cards) and non-IT countermeasures (such as guards and procedures). ” [2, p. 39, Part 1: Introduction and general model]. The standard uses the term countermeasure for security control.
Vulnerability and Threat Analysis
The common criteria considers threats from malicious attackers and also from attackers that present unintentional threats such as accidental disconnecting a server from a power supply. “The Common Criteria is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. ” [2, p. 16 and p. 20, Part 1: Introduction and general model]. The common criteria suggests further to describe the *attack potential* that “measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker’s expertise, resources and motivation. ” [2, p. 14, Part 1: Introduction and general model]. The description of attackers leads to threats the attacker present by exploiting vulnerabilities.
Risk Determination
The Common Criteria focuses on identifying vulnerabilities and attackers that might exploit these vulnerabilities. “These threats therefore give rise to risks to the assets, based on the likelihood of a threat being realised and the impact on the assets when that threat is realised. ” [2, p. 39, Part 1: Introduction and general model]. However, the standard does not follow a risk management approach like ISO 31000, but focuses on documenting vulnerabilities and countermeasures of a TOE. An ST shall help to decide if a stakeholder is willing to accept the risk of using a TOE. “Once an ST and a TOE have been evaluated, asset owners can have the assurance (as defined in the ST) that the TOE, together with the operational environment, counters the threats. The evaluation results may be used by the asset owner in deciding whether to accept the risk of exposing the assets to the threats. ” [2, p. 58, Part 1: Introduction and general model].

Table 11. Instantiation for Common Criteria of the Security Analysis Product Part of the Template for Security Standard Description (1/2)

Security Analysis Product
Security Assessment
Each of the threats previously identified leads to the formulation of a *security objective*, which is equal to a security requirement in the common terminology. The Common Criteria distinguishes between security objectives, which concern the TOE, and the ones concerning the environment. The latter ones are so-called *security objectives for the environment*. Moreover, the Common Criteria considers organization security policies, which are equal to the policy term. The Common Criteria uses cross-tables that present a mapping of all identified threats to security objectives, security objectives for the environment, assumptions, or organization security policies. Each threat has to mapped to at lease one security objectives, security objectives for the environment, or assumptions.
Security Measures
Security objectives are refined by security functional requirements, which are gap texts that concern specific security functions such as access control functions. Security objectives are on a high abstraction level, while security functional requirements concern concrete implementable security functionalities. All security objectives have to be refined using security functional requirements. A cross-table has to show that all security objectives are refined by at least one security functional requirement.
Risk Acceptance
"Owners of assets may be (held) responsible for those assets and therefore should be able to defend the decision to accept the risks of exposing the assets to the threats. " [2, p. 39, Part 1: Introduction and general model].

Table 12. Instantiation for Common Criteria of the Security Analysis Product Part of the Template for Security Standard Description (2/2)

Security Analysis Product
Security and Risk Documentation
The concepts of the Common Criteria consider that potential ToE owners infer their security needs for specific types of ToE, e.g., a specific database. The resulting documents are called Security Targets (ST). Protection profiles (PP) state security needs for an entire class of ToEs, e.g., client VPN application. The evaluators check if a ToE meets its ST. PPs state the security requirements of ToE owners. ToE developers or vendors publish their security claims in an ST. A CC evaluation determines if the ST is compliant to a specific PP. The standard relies upon documents for certification, which state information about security analysis and taken measures. The structure of a CC security target starts with an ST *Introduction* that contains the description of the ToE and its environment. The *Conformance Claims* describe to which PPs the ST is compliant. The *Security Problem Definition* refines the external entities, e.g., stakeholders in the environment and lists all assets, assumptions about the environment and the ToE, threats to assets and organizational security policies. The *Security Objectives* have to be described for the ToE and for the operational environment of the ToE. The *Extended Component Definitions* describe extensions to security components described in the CCs part 2. The *Security Requirements* contain two kinds of requirements. The security functional requirements (SFR) are descriptions of security functions specific to the ToE. The security assurance requirements (SAR) describe the measures taken in development of the ToE. These are evaluated against the security functionality specified in the SFR. The Evaluation Assurance Level (EAL) is a numerical rating ranging from 1 to 7, which states the depth of the evaluation. Each EAL corresponds to an SAR package. EAL 1 is the most basic level and EAL 7 the most stringent. The Common Criteria defines a set of *Security Assurance Components* that have to be considered for a chosen *Evaluation Assurance Level (EAL)*. For these components, developer activities, content of corresponding components, and actions for an evaluator are defined. The Common Criteria defines security assurance components for the following *Assurance classes*: – Protection Profile Evaluation (APE) – Security Target Evaluation (ASE) – Development (ADV) – Life-Cycle support (ALC) – Tests (ATE) – Vulnerability Assessment (AVA) In the Security Target, Security Objectives are defined for the TOE on for the TOE's environment. The Security Objectives are related to Security Functional Requirements. Part of the assurance classes for the development documentation (ADV) is the functional specification (ADV_FSP). In this document, the security functions (SFs) are defined. According to the security architecture (as required in ADV_ARC), the TOE design with details about the subsystems and modules are documented in the TOE design (ADV_TDS). This design document brakes down the security functions (SFs) and relates all subsystems and modules to the security functional requirements (SFRs) they implement. Vulnerabilities are assessed in the corresponding document according to the claimed attack potential (high, medium, low)(AVA_VAN).

7 CAST Step 5: Compare Standards

We analyze the instantiated templates (Sect. 6) of the ISO 27001 standard (Sect. 6.1), IT Grundschutz (Sect. 6.2), and Common Criteria (Sect. 6.3) in Sect. 7.1. In addition, we describe the tool support for our method in Sect. 7.2.

7.1 Comparison

We compared the terminology of the security standards ISO 27001, IT Grundschutz, and Common Criteria in Tab. 7.1 with the terminology introduced in Sect. 3. The symbol ”∼“ means that the term is equal to the definition in our terminology (Sect. 3). A ”−“ states that the standard does not consider that term explicitly.

Table 13. Term Comparison between Security Standards

terms \standards	**ISO 27001**	**IT Grundschutz**	**Common Criteria**
machine	ISMS	ISMS	TOE
environment	outside the boundaries of the ISMS	interfaces to external partners	operational environment
stakeholder	interested parties	employees and users	TOE owner, users
asset	∼	∼	∼
security control	controls	safeguards	countermeasure
attacker	-	-	threat agent
vulnerability	∼	∼	∼
threat	∼ *	∼ *	∼
policy	ISMS policy, security policy	information security policy	organizational security policy
security goals	security objectives	protection requirements	security needs
security requirements	∼	(security test plans)**	security objective
security functions	-	-	security functional requirements

* Note that attackers can be seen as threats.

** Note that the security test plan are not requirements, but are based on refined protection requirements.

Furthermore, we show the results of our comparison in the following by illustrating relevant statements for each of our building blocks of our security standard template instances.

Security Analysis Context and Preparation

Environment description - The ISO 27001 demands a scope definition including assets and justifications. The standard refers explicitly to use the scope in subsequent steps such as risk identification. Moreover, the scope is also referred to in the documented management commitment. The IT Grundschutz demands also explicitly to document external partners and to document certain parts of the scope separately, such as applications. The Common Criteria focuses on functionalities of the TOE and its environment in the scope description.

Stakeholder description - The ISO 27001 demands stakeholder description as part of the scope description including their security expectations. The IT

Grundschutz considers all employees and external staff involved in relevant business processes as stakeholders. The Common Criteria concerns all users of the TOE as stakeholders.

Asset identification - ISO 27001 demands the definition of assets, but does not provide methodological support for it. The IT Grundschutz considers all information technology and information in the business processes as assets. The Common Criteria considers also the concept of a secondary assets. But the standard does not provide a method for identifying them, either.

Risk level determination - The ISO 27001 demands a high level risk definition in alignment with the risk management of the organization. The IT Grundschutz standards use protection requirements as high level risk indicators. The Common Criteria standard does not consider high level risks, but it does define attack potentials.

Security Analysis Process

Risk Determination - The ISO 27001 demands a description of the risk management methodology. The IT Grundschutz proposes a categorization of assets and to conduct a risk analysis only for the assets with significant security concerns. The standard does not demand a specific method for risk management, but it provides advice for considering risk, threats, and security controls. The Common Criteria focuses on documenting vulnerabilities and security controls of the TOE. It does not consider risk management per se, but rather provides the information about threats and countermeasures to stakeholders. Afterwards the stakeholders can use this information to conduct a risk analysis.

Security Property Description - ISO 27001 demands high level security goals as part of the ISMS policy, which defines the focus of security of the ISMS and is described right after the scope. The IT Grundschutz demands to describe protection requirements using confidentiality, integrity, and availability. In addition, the standard demands a categorization into the levels: normal, high, very high. The Common Criteria demands that security concerns are described in terms of confidentiality, integrity, and availability. The standard contains a catalog of refinements of these terms, which have to be used in TOE descriptions.

Control Assessment - The ISO 27001 focuses on likelihoods of threats exploiting existing vulnerabilities and the effect already implemented controls have on these likelihoods. The IT Grundschutz has mappings from threats to security controls and it has to be checked if the recommended security controls are implemented for all identified threats. The Common Criteria documents existing security controls by describing existing security functionalities of the TOE. The gap texts in the security functional requirements of the standard have to be used for these descriptions.

Vulnerability and Threat Analysis - The ISO 27001 concerns threat analysis in order to determine risks for assets. The threat analysis is based on a vulnerability identification. The IT Grundschutz standard relies on a list of threats for the identified scope parts, e.g., applications from the IT Grundschutz Catalogues. The Common Criteria demands to describe threats from malicious and from unintentional attackers. The capabilities of these attackers have to be described in terms of expertise, resources, and motivation.

Security Analysis Product

Security Assessment - The ISO 27001 demands to evaluate the risks to assets considering threats and existing security controls. For all assets with unacceptable risks, additional security controls have to be selected from the normative ANNEX A of the standard. The IT Grundschutz standards begin with a basic security check, which is based on security tests derived from the protection requirements. The tests are used for an effectiveness evaluation of the existing security controls. The Common Criteria relies on cross-tables that map threats to security objectives. All threats have to be addressed by at least one security objective or assumption.

Security Measures - The ISO 27001 demands first high level security policies, which are refined into a set of relevant security controls considering the controls listed in the mandatory ANNEX A of the standard. The IT Grundschutz demands using the mapping from scope elements to threats, and subsequently to security controls in the IT-Grundschutz Catalogues. Only assets that are not considered adequately in the IT-Grundschutz Catalogues demand a separate security analysis. The Common Criteria refines security objectives using a catalog of security functional requirements. A further cross-table has to proof that each security objective is addressed by at least one security functional requirement.

Risk Acceptance - The ISO 27001 demands to define criteria for risk acceptance in the management approval document. The standard demands a reasoning why the selected security controls reduce the risk to acceptable limits for each asset. The IT Grundschutz simply demands a documentation of accepted risks including a reason why these risks are accepted. The Common Criteria demands risk acceptance decisions from asset owners. They have to make an informed decision to accept the risks of the identified threats.

Security and Risk Documentation - The ISO 27001 demands documentation about the scope and security policies, and extensive documentation of the risk management. The IT Grundschutz standards simply demand to document all the steps of the method. The Common Criteria demands an extensive documentation of the security reasoning and the resulting software product, and in particular the security functions of the product.

To sum up, the ISO 27001 concerns a high level process with regard to security. The IT Grundschutz refines the ISO 27001 process and provides further guidances for identifying threats and security controls based on the IT Grundschutz Catalogues. In contrast, the Common Criteria focuses on documenting a software or hardware product including details of its implementation. The reasoning about which security standard is applicable should be based on the concerned application domain. A vendor of a hardware router might want to select the Common Criteria, due to the detailed security analysis of its implementation. A cloud computing provider who offers scalable IT resources and particular business processes concerning these resources might favor ISO 27001. A reason could be that documenting a high level security process allows changes within the cloud implementation, because the process does not consider the implementation in detail. Using the Common Criteria would demand a documentation of its implementation and a re-certification each time the implementation changes.

7.2 CAST Tool Support

We base our tool support on the NESSoS CBK (Sect. 2) that aims to collect knowledge on engineering secure systems. The structure of the *CBK* relates Knowledge Objects (KOs) for specific fields (referred to as Knowledge Areas – KAs). We define the following four types of KOs. *Methods* define a set of activities used to tackle problems in engineering secure software and services in a systematic way. *Techniques* describe an approach that contains only a single activity. *Tools* support a software engineer in achieving a development goal in an (at least partially) automated way. A *Notation* defines symbols, a syntax, and semantics to express relevant artifacts [30]. We included security standards as a fifth type of KO, meaning we implemented the security standard template in its underlying ontology. In addition, the CBK offers the functionality to compare KOs by displaying their attributes next to each other. Hence, we can display two instantiated security standard templates next to each other. This way the comparison of them is supported. Furthermore, a search functionality allows to search the instantiated templates for specific search terms. In the future, we are planning to implement an automatic search for supporting KOs for security standards and a comparison of security standard support methodologies.

7.3 Discussion

Our method provides the means to describe three building blocks of security standards. The first block states how context description and preparation of a security analysis has to be done in a standard. This provides an overview of the level of detail demanded for a security standard compliant system documentation. For example, the IT-Grundschutz standards demand to treat every item in the scope as an asset and conduct a security analysis for it, while the ISO 27001 demands a reasoning about which are the assets in the scope. Hence, the ISO 27001 allows more flexibility in the security analysis.

The security analysis process shows how existing controls, risk, threats and vulnerabilities have to be analyzed. For example, the IT-Grundschutz demands a characterization of the existing controls according to certain categories, while the ISO 27001 simply refers to a statement of how the existing controls reduce the likelihoods of security failures. This is another indication that the ISO 27001 demands a less structured documentation than the IT-Grundschutz standards. In contrast, the Common Criteria controls are clearly separated into IT and non-IT countermeasures. For this reason, the standard can be applied especially for product development.

Finally, the security analysis product shows the overall security assessment and in particular how security measures have to be described, risk acceptance to be determined, and what documentation is required for a certification. As an

example, the ISO 27001 demands a specific set of a few documents, while the IT-Grundschutz simply demands to document the entire process.
Our method creates the following main benefits:

- A simple overview of the core activities of security standards.
- Enabling a structured comparison of standard activities by storing the knowledge about standards in defined template fields.
- Providing indication of the focus, level of detail, and effort for providing or even reading a system documentation according to a specific standard.

We could identify the following points for improvement of our work:

- The approach could be extended to compare also support tools for standard compliant system documentation and analysis
- Our templates can be analyzed for re-using artifacts and results of the certification of one standard for another. This could lead to a possible optimal sequence of certifications of different standards with regard to resources spent in terms of time and money.
- The overview is provided on an abstract level and the engineers still have to read the standards to compare these on a more granular level. Our method could be extended to support a more detailed analysis of the standard documents.

8 Related Work

To the best of our knowledge, no structured method exists to compare security standards using a conceptual model, template and a common terminology.

The U.S. Department of Energy compared the ISO/IEC 17799, NIST PC-SRF, ISA-TR99.00.01-2004 and ISA-TR99.00.02-2004 security standards [31]. The authors compare terms and notions of the standards, but they do not rely on a conceptual model or template.

Siponen and Willison [32] analyzed to which kinds of organizations the standards and guidelines BS7799, BS ISO/IEC17799: 2000, GASPP/GAISP, and the SSE-CMM are helpful. They do not compare notions, concepts or terminology.

Sommestad et al. [33] compare standards for Cyber security of Supervisory Control And Data Acquisition (SCADA). SCADA systems are crucial for critical infrastructures, e.g., electrical power system. Sommestad et al. compare a number of SCADA standards and the ISO 27002 standard. The authors compare the sets of threats and countermeasures stated in the standards. Sommestad et al. divide the standards into those that focus on technical countermeasures and those that focus on organizational countermeasures and analyze their commonalities and differences. This research can complement our own by refining our building block that concerns countermeasures using their results.

Phillips et al. [34] analyze security standards for the RFID market: ISO/IEC 15693, ISO/IEC 10536, ISO/IEC 11784-11785, ISO/IEC 18000-3, ISO/IEC 18000-2. The authors list the availability, integrity, and confidentiality demands of these standards. Their aim is to provide a complete set of security goals for the RFID market and not to compare the standards.

Kuligowski [35] compares the FISMA security standards and the ISO 27001 standard by comparing terminology and mapping their activities. The work does not provide a common terminology or conceptual model that could be applied to further standards.

NIST [36] compares the standards FIPS 140-1 AND FIPS 140-2 regarding their specification of cryptographic modules. The authors also compare terminologies and description of cryptographic functionalities. This work does not aim at creating a terminology or conceptual model for security standards.

Arora [37] compares the ISO 27001 and the COBIT standard using a template that contains the fields: focus, paradigm, scope, structure, organizational model, and certification. The author does not provide a conceptual model or terminology comparison. Moreover, the template is lacking a detailed focus on security and risk management activities.

The government of Hong Kong released a report about security standards [38]. The report provides summaries of the standards ISO 27001, ISO 27002, COBIT, ITIL, etc. and also legal norms such as SOX and HIPAA. The report is not comparing the standards, but just aims at providing easily readable introductions into these standards. Hence, the report does not provide terminology comparisons, conceptual models, or templates.

9 Conclusion and Future Work

We contributed a conceptual model of security standards based on existing research such as the HatSec method and the NIST SP 800-30 standard. Furthermore, we derived a template from the conceptual model that can be instantiated for different security standards. We applied this idea to several security standards and compared the resulting template instances.

Our approach offers the following main benefits:

- A structured method for comparing security standards.
- A common terminology and a conceptual model of security standards
- A template that supports the structured collection of knowledge by using common security standard activities, e.g., asset identification
- A set of instantiated security standard templates for the standards ISO 27001, IT Grundschutz, and Common Criteria. The templates provide an overview of the most relevant standard activities.
- Improving the understanding of commonalities and differences of security standards by analyzing the difference in the common standard activities, e.g., how do ISO 27001 and Common Criteria identify assets?
- Supporting security engineers in the decision which certification scheme to pursue and what kind of information to expect from a security standard documentation.
- Providing tool support for the comparison of security standards.

In the future, we will compare further standards and include also the comparison of risk management standards such as ISO 31000. In addition, we will extend the common terminology and also add a change template specifically designed to compare different versions of a standard.

References

1. International Organization for Standardization (ISO), International Electrotechnical Commission (IEC): Information technology - Security techniques - Information security management systems - Requirements (2005)
2. ISO/IEC: Common Criteria for Information Technology Security Evaluation. ISO/IEC 15408, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2012)
3. ISO/IEC: Risk management — Principles and guidelines. ISO/IEC 31000, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) (2009)
4. Sunyaev, A.: Health-Care Telematics in Germany - Design and Application of a Security Analysis Method. Gabler (2011)
5. für Sicherheit in der Informationstechnik (BSI), B.: Standard 100-3 Risk Analysis based on IT-Grundschutz, Version 2.5 (2008)
6. JASON: Science of Cyber-Security. Technical report, The MITRE Corporation (2010) JSR-10-102.
7. Stoneburner, G., Goguen, A., Feringa, A.: Risk management guide for information technology systems. NIST Special Publication 800-30, National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8930 (July 2002)
8. Beckers, K., Eicker, S., Faßbender, S., Heisel, M., Schmidt, H., Schwittek, W.: Ontology-based identification of research gaps and immature research areas. In: Proceedings of the International Cross Domain Conference and Workshop (CD-ARES 2012). Lecture Notes in Computer Science, Springer (2012) 1–16
9. Fabian, B., Gürses, S., Heisel, M., Santen, T., Schmidt, H.: A comparison of security requirements engineering methods. Requirements Engineering – Special Issue on Security Requirements Engineering **15**(1) (2010) 7–40
10. Jackson, M.: Problem Frames. Analyzing and structuring software development problems. Addison-Wesley (2001)
11. Gollmann, D.: Computer Security. 2nd edn. John Wiley & Sons (2005)
12. Bishop, M.: Computer Security : art and science. 1st edn. Pearson (2003)
13. Viega, J., McGraw, G.: Building secure software: how to avoid security problems the right way. 1st edn. Addison-Wesley (2001)
14. Firesmith, D.: Common concepts underlying safety, security, and survivability engineering. Technical report sei-2003-tn-033, Carnegie Melon University (2003)
15. ISO/FDIS: ISO/IEC 27799:2007(E), Health Informatics - Information Security Management in health using ISO/IEC 27002 (November 2007)
16. Stallinger, M.: CRISAM - Coporate Risk Application Method - Summary V2.0 (2004)
17. Farquhar, B.: One approach to risk assessment. Computers and Security **10**(10) (February 1991) 21–23
18. Karabacak, B., Sogukpinar, I.: Isram: information security risk analysis method. Computers & Security **24**(2) (2005) 147 – 159

19. Japan Information Processing Development Corporation and The Medical Information System Development Center: ISMS User's Guide for Medical Organizations (2004)
20. Standards Australia International; Standards New Zealand: Guidelines for managing risk in healthcare sector: Australian/ New Zealand handbook (2001) Standards Australian International.
21. Food, Administration, D.: Guideline for Industry, Q9 Quality Risk Management (2006) In US Department of Health and Human Services.
22. ISO/IEC: ISO/IEC 27005:2007, Information technology - Security techniques - Information security risk management (November 2007)
23. DCSSI: Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) - Section 2 - Approach. General Secretariat of National Defence Central Information Systems Security Division (DCSSI) (February 2004)
24. Sharp, H., Finkelstein, A., Galal, G.: Stakeholder identification in the requirements engineering process. In: DEXA Workshop. (1999) 387–391
25. Pouloudi, A.: Aspects of the stakeholder concept and their implications for information systems development. In: HICSS. (1999)
26. für Sicherheit in der Informationstechnik (BSI), B.: Standard 100-1 Information Security Management Systems (ISMS), Version 1.5 (2008)
27. BSI: IT-Grundschutz-Vorgehensweise. BSI standard 100-2, Bundesamt für Sicherheit in der Informationstechnik (BSI) (2008)
28. BSI: BSI Standard 100-4 Business Continuity Management, Version 1.0. BSI standard 100-4, Bundesamt für Sicherheit in der Informationstechnik (BSI) (2009)
29. BSI: Protection Profile for the Gateway of a Smart Metering System (Gateway PP). Version 01.01.01(final draft), Bundesamt für Sicherheit in der Informationstechnik (BSI) - Federal Office for Information Security Germany, Bonn,Germany (2011) `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/SmartMeter/PP-SmartMeter.pdf?__blob=publicationFile`.
30. Schwittek, W., Schmidt, H., Eicker, S., Heisel, M.: Towards a Common Body of Knowledge for Engineering Secure Software and Services. In: Proceedings of the International Conference on Knowledge Management and Information Sharing (KMIS), SciTePress - Science and Technology Publications (2011) 369–374
31. U.S. Department of Energy: A comparison of cross-sector cyber security standards. Technical report, Idaho National Laboratory (2005)
32. Siponen, M., Willison, R.: Information security management standards: Problems and solutions. Inf. Manage. **46**(5) (June 2009) 267–270
33. Sommestad, T., Ericsson, G., Nordlander, J.: Scada system cyber security; a comparison of standards. In: Power and Energy Society General Meeting, 2010 IEEE. (july 2010) 1 –8
34. Phillips, T., Karygiannis, T., Kuhn, R.: Security standards for the rfid market. Security Privacy, IEEE **3**(6) (nov.-dec. 2005) 85 – 89
35. Christine Kuligowski: COMPARISON OF IT SECURITY STANDARDS. Technical report, (2009) `http://www.federalcybersecurity.org/CourseFiles/WhitePapers/ISOvNIST.pdf`.
36. NIST: A COMPARISON OF THE SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES IN FIPS 140-1 AND FIPS 140-2. Nist special publication 800-29, National Institute of Standards and Technology (NIST), Gaithersburg, United States (2001) `http://csrc.nist.gov/publications/nistpubs/800-29/sp800-29.pdf`.

37. Varun Arora: Comparing different information security standards: COBIT vs. ISO 27001. Technical report, Carnegie Mellon University, Qatar, United States (2010) `http://qatar.cmu.edu/media/assets/CPUCIS2010-1.pdf`.

38. HKSAR: AN OVERVIEW OF INFORMATION SECURITY STANDARDS. Technical report, The Government of the Hong Kong Special Administrative Region (HKSAR), Hong Kong, China (2008) `http://www.infosec.gov.hk/english/technical/files/overview.pdf`.

Appendix

A Template for Security Standards

Table 14. Security Analysis Context and Preparation Part of the Template for Security Standard Description

Security Analysis Context and Preparation
Environment Description
– Which essential parts of the environment have to be described? – How do relations between these parts have to be described? – What is the required abstraction level of the description? **Relevant common terms:** *machine, environment*
Stakeholder Description
– How are stakeholders defined? – Which relation to the machine is required to be a stakeholder? – Are there restrictions on stakeholders, e.g., do they have to be humans? **Relevant common terms:** *stakeholder*
Asset Identification
– How are assets identified? – Which relation does a stakeholder have to an asset? – Are assets categorized? **Relevant common terms:** *asset*
Risk Level Definition
– What kinds of risk levels are defined? – What is the required abstraction for these risk levels? – How do the risk levels relate to assets and stakeholders?

Table 15. Security Analysis Process Part of the Template for Security Standard Description

Security Analysis Process
Security Property Description
– Do specific security goals have to be considered for assets, e.g., confidentiality? – Which further security properties are used and how are they defined? – What kind of methodology is required to elicit security goals? **Relevant common terms:** security goal, availability, confidentiality, integrity
Control Assessment
– How are existing security controls identified? – Is it mandatory to described the threats that existing controls mitigates? – Is it required to describe which assets an existing control protects? **Relevant common terms:** security control
Vulnerability and Threat Analysis
– What kind of attacker model does the standard consider? – Which activities does the standard demand for threat and vulnerability analysis? – When is the threat and vulnerability analysis complete? **Relevant common terms:** attacker, vulnerability, threat
Risk Determination
– How is risk defined e.g. as a product of likelihoods and consequences? – Is a process for risk management defined? – Is a qualitative or quantitative risk determination required?

Table 16. Security Analysis Product Part of the Template for Security Standard Description

Security Analysis Product
Security Assessment
– How are controls selected? – Does a categorization exist for controls, e.g., types of threats the controls protect against? – Do relations between controls have to be considered, e.g., one control has a working access control as a precondition? **Relevant common terms:** security requirements, policies
Security Measures
– What criteria are used to determine that a control is relevant to mitigate a particular threat? – Is there a demand to describe the improved protection these controls provide? – How is the reasoning done that the selected controls are sufficient and no further controls are required? **Relevant common terms:** security functions, policies
Risk Acceptance
– How are acceptable risk levels defined? – Which kind of assessment determines that a security control reduces the risk to an acceptable risk? – What kind of review is required to ensure that the risk is acceptable?
Security and Risk Documentation
– What methods are used to document the results e.g. templates, check lists? – What kind of documents are required for certification? – Can documents from other certifications be re-used?