Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing

Kristian Beckers, Holger Schmidt
Faculty of Engineering – Department of Computational and Applied Cognitive Science
University Duisburg-Essen, Germany
Email: {Kristian.Beckers, Holger.Schmidt}@uni-duisburg-essen.de

Jan-Christoph Küster
Fraunhofer ISST, Germany
Email: {Jan-Christoph.Kuester}@isst.fraunhofer.de

Stephan Faßbender
Faculty of Computer Science
TU Dortmund, Germany
Email: {Stephan.Fassbender}@cs.tu-dortmund.de

***Abstract*—The ISO 27000 is a well-established series of information security standards. The scope for applying these standards can be an organisation as a whole, single business processes or even an IT application or IT infrastructure. The context establishment and the asset identification are among the first steps to be performed. The quality of the results produced when performing these steps has a crucial influence on the subsequent steps such as identifying loss, vulnerabilities, possible attacks and defining countermeasures. Thus, a context analysis to gather all necessary information in the initial steps is important, but is not offered in the standard.**

In this paper, we focus on the scope of cloud computing systems and present a way to support the context establishment and the asset identification described in ISO 27005. A *cloud system analysis pattern* and different kinds of *stakeholder templates* serve to understand and describe a given cloud development problem, i.e. the envisaged IT systems and the relevant parts of the operational environment. We illustrate our support using an online banking cloud scenario.

***Keywords*-security standards; cloud computing; requirements engineering.**

I. Introduction

Cloud computing offers highly flexible and scalable usage of IT resources, from which companies can benefit. The International Data Corporation study from 2009[1] identifies security as a significant barrier for the acceptance of clouds in companies. In order to gain their customers *trust*, companies have to achieve an acceptable security level, if using clouds. Security standards such as the *ISO 27000 series of standards*, also known as 2700x, offer a way to attain this goal. Consequently, we consider in this paper the application of the ISO 2700x in the field of cloud computing systems. We focus on the scope and boundaries part [1, Clause 7.3] of the context establishment [1, Clause 7] and the identification of assets [1, Clause 8.2.1.2] of the ISO 27005. These steps are difficult to execute, due to the sparse description. As the input needed to define scope and boundaries, the standard simply demands "all information about the organisation relevant to the information security risk management context establishment" [1, Clause 7.1].

The importance of these steps becomes obvious, when one realises that essential further steps of the ISO 27005 depend upon them, e.g. threat identification, identification of existing controls, and identification of vulnerabilities. Thus, mistakes in the context establishment, and asset identification can result in great loss.

We present a *pattern for analysing clouds*, which is complemented by templates to elicit knowledge about the different stakeholders contained in the pattern. We then describe how the pattern and especially the stakeholder templates can be used to support the ISO 27005 activities of context establishment and asset identification.

Running Example: we illustrate our pattern-based support for security standards, using the example of a bank offering an online-banking service for their customers. This bank plans to source out the affected IT processes to reduce costs and scale up their system for a broader amount of customers. Customer data such as account number, amount, and transaction log history are stored in the cloud, and transactions like credit transfer are processed in the cloud. The bank authorises the software department to design and build the cloud-specific software according to the interface and platform specification of the cloud provider.

The rest of the paper is organised as follows: Section II presents background on clouds and the ISO 2700x standards, especially the ISO 27005. We introduce a pattern for analysing cloud computing systems in Sect. III. In Sect. IV, we show how this pattern can be used to support the context establishment and asset identification steps. We consider related work in Sect. VI. In Sect. VII, we give a summary and directions for future research.

II. Background

In Sect. II-A, we describe the main characteristics of clouds. In Sect. II-B, we present a short survey about the ISO 2700x standards for information security and especially

[1] https://www-304.ibm.com/isv/library/pdfs/cloud_idc.pdf

explain the information security risk management process described in ISO 27005.

A. Cloud Computing Systems

The term *cloud computing* describes a technology as well as a business model [2]. According to the *National Institute of Standards and Technology (NIST)* cloud computing systems can be defined by the following properties [3]: the cloud customer can require resources of the cloud provider over *broad network access* and *on-demand* and pays only for the used capabilities. Resources, i.e., storage, processing, memory, network bandwidth, and virtual machines, are combined into a so-called *pool*. Thus, the resources can be virtually and dynamically assigned and reassigned to adjust the customers' variable load and to optimise the resource utilization for the provider [4]. The virtualisation causes a location independence: the customers generally have no control or knowledge over the exact location of the provided resources. The resources can be quickly scaled up and scaled down for customers and appear to be unlimited, which is called *rapid elasticity*. The pay-per-use model includes guarantees such as availability or security for resources via customized *Service Level Agreements (SLA)* [4].

The architecture of a cloud computing system consists of different service layers and allows different business models: On the layer closest to the physical resources, the *Infrastructure as a Service (IaaS)*, are provided pure resources, for instance virtual machines, where customers can deploy arbitrary software including an operating system. Data storage interfaces provide the ability to access distributed databases on remote locations in the cloud.

On the *Platform as a Service (PaaS)* layer, customers use an API to deploy own applications using programming languages and tools supported by the provider. On the *Software as a Service (SaaS)* layer, customers use applications offered by the cloud provider that are running on the cloud infrastructure. Furthermore, cloud providers require a layer that monitors their customers' resource usage, e.g. for billing purposes and service assurances. Buyya et al. [5] introduce this layer as a middleware in their cloud model.

Cloud computing offers different usage scenarios: *private clouds* are operated solely for an organization, *public clouds* are made available to the general public or a large industry group and are owned by a third party selling cloud services. In between these scenarios are *hybrid clouds* where users complement internal IT resources upon demand with resources from an external vendor [2].

B. ISO 27000 Series of Standards

The ISO 27000 is an international and a well known series of standards to deal with information security and is relevant for all types of organizations, e.g. commercial enterprises, government agencies, non-profit organizations. The ISO 27001 contains the specification for an *information security management system (ISMS)*, the ISO 27002 outlines potential controls and control mechanisms for reducing risks, the ISO 27004 covers information security system management measurement and metrics, and the ISO 27005 states a methodology independent ISO standard for information security risk management. The ISO 27006 provides guidelines for the accreditation of organizations offering ISMS certification and the ISO 27003 is a so far unreleased standard, that will offer guidance for the implementation of an ISMS. The section of the standards are named clauses.

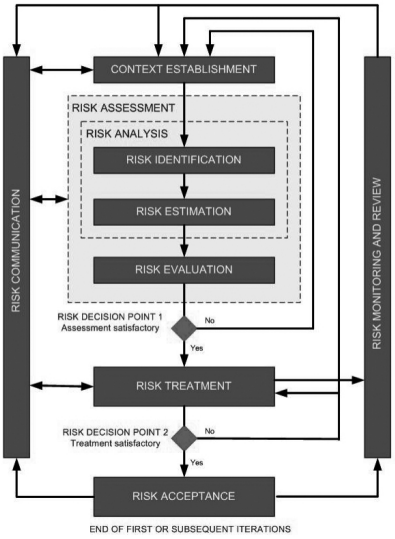

Figure 1. Information Security Risk Management Process (taken from [1])

In this section we describe the information security risk management process of Clause 6 in the ISO 27005 more detailed to focus in the subsequent part of this paper on how to support this process with our cloud system analysis pattern for cloud scenarios. Figure 1 shows the information security risk management process, that consists of activities, i.e. steps, depicted in the dark grey boxes. For each activity the standard documents the *input*, the *action* with a corresponding *implementation guidance* and the *output*.

The process starts with the activity of *context establishment*. In a sub step, it defines amongst others the *scope and boundaries*, that "consists of assets that should be identified and described" and that "ensures that all relevant assets are taken into account in the risk management". As mentioned in Sect. I, this initial step is important for all following steps and is responsible, whether the risk management can be implemented in a sufficient extent and on a sufficient level of detail. Beside the scope, the context establishment includes defining other general information for the process, e.g. the general levels of risk acceptance of the organization or the responsibilities of the organization for the risk management.

The next step is the *risk identification*, that determine po-

tential loss. Therefore sub steps are *identification of assets*, that takes the scope and boundaries as input, *identification of threats* on the asset and *identification of consequences*, that loss has on the assets. Then *risk estimation* tries to rate the consequences of loss on a qualitative or quantitative scale as well as the likelihood of occurrence. The *risk evaluation* step compares the level of risks against the risk acceptance criteria, defined during the context establishment. Then, the *risk treatment* step sets up controls, that are described in detail in ISO 27002, to reduce the risk to an acceptable level of residual risk. In the *risk acceptance* step, residual risks have to be accepted by managers of the organization. The *risk communication* is important through the whole process and ensures awareness of risks and the controls in place by managers and all other employees. Finally, the *risk monitoring and review* activity controls and reflect the results of the process that are used continually as new input for the process.

The German *BSI standard 100-2* also describes how an ISMS can be established and managed. It is compatible to the ISO 27001 standard and is a national implementation of the international ISO standard. That means BSI standard 100-2 can be used for an ISO 27001 certification [6].

III. Pattern-Based Cloud Analysis

We present in Sect. III-A a cloud system analysis pattern that helps to systematically perform requirement analyses in the field of cloud computing. Then, in Sect. III-B, we illustrate the instantiation of the pattern using the online banking service example.

A. Cloud System Analysis Pattern

We present a *cloud system analysis pattern* in Fig. 2 that provides a conceptual view on cloud computing systems and serves to systematically analyse stakeholders and requirements. The notation used to specify the pattern is based on UML[2] notation, i.e. the stick figures represent roles, the boxes represent concepts or entities of the real world, the named lines represent relations (associations) equipped with cardinalities, the unfilled diamond represents a "part-of" relation, and the unfilled triangles represent inheritance.

A Cloud is embedded into an environment consisting of two parts, namely the Direct System Environment and the Indirect System Environment. The Direct System Environment contains stakeholders and other systems that directly interact with the Cloud, i.e. they are connected by associations. Moreover, associations between stakeholders in the Direct and Indirect System Environment exist, but not between stakeholders in the Indirect System Environment and the cloud. Typically, the Indirect System Environment is a significant source for compliance and privacy requirements.

The Cloud Provider owns a Pool consisting of Resources, which are divided into Hardware and Software resources. The

[2]Unified Modeling Language: http://www.omg.org/spec/UML/2.3/

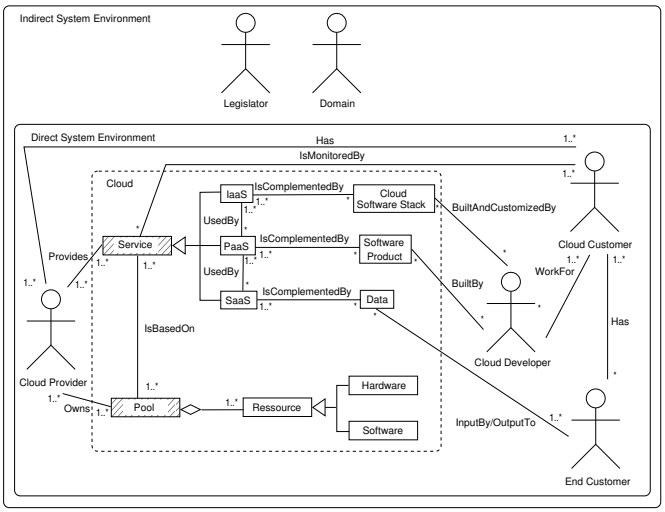

Figure 2. Cloud System Analysis Pattern

provider offers its resources as Services, i.e. IaaS, PaaS, or SaaS. The boxes Pool and Service in Fig. 2 are hatched, because it is not necessary to instantiate them. Instead, the specialised cloud services such as IaaS, PaaS, and SaaS and specialised Resources are instantiated. The Cloud Developer represents a software developer assigned by the Cloud Customer. The developer prepares and maintains an IaaS or PaaS offer. The IaaS offer is a virtualised hardware, in some cases equipped with a basic operating system. The Cloud Developer deploys a set of software named Cloud Software Stack (e.g. web servers, applications, databases) into the IaaS in order to offer the functionality required to build a PaaS. In our pattern PaaS consists of an IaaS, a Cloud Software Stack and a *cloud programming interface (CPI)*, which we subsume as Software Product. The Cloud Customer hires a Cloud Developer to prepare and create SaaS offers based on the CPI, finally used by the End Customers. SaaS processes and stores Data in- and output from the End Customers. The Cloud Provider, Cloud Customer, Cloud Developer, and End Customer are part of the Direct System Environment. Hence, we categorise them as *direct stakeholders*. The Legislator and the Domain (and possibly other stakeholders) are part of the Indirect System Environment. Therefore, we categorise them as *indirect stakeholders*.

We accompany this cloud system analysis pattern by templates to systematically gather domain knowledge about the direct and indirect system environments based upon the stakeholders' relations to the cloud and other stakeholders. The first template serves to describe stakeholders contained in the direct system environment:

Name State the identifier of the stakeholder or group of stakeholders, e.g. company name or group of end customers.

Description Describe the stakeholder informally, e.g. if the stakeholder is a natural or a legal person.

Relations to the cloud Describe the inputs and outputs represented as relation (line from this stakeholder to the cloud) between the stakeholder and the cloud, e.g. the kind of data or software.

Motivation State the motivation of the stakeholder for using the cloud based on the previous considered relations to the cloud, e.g. business goals such as profit and costs reduction.

Relations to other direct stakeholders For each relation (line from this stakeholder to another direct stakeholder), name the kind of dependency between the stakeholders, e.g. controlled by contract, served by, indirectly influenced by customer-demand.

Assets Identify the assets relevant for this stakeholder, e.g. by considering the relations to the cloud.

Compliance and Privacy Identify relevant compliance and privacy laws as well as regulations based on the indirect stakeholders. Specify and identify the ones relevant for the stakeholder at hand, e.g. BDSG.

The second template serves to describe stakeholders contained in the indirect system environment:

Name See direct stakeholder template.

Description See direct stakeholder template.

Relations to other stakeholders For each relation from this stakeholder to another direct or indirect stakeholder (no line explicitly shown), name the kind of dependency between the stakeholders, e.g. protected by, controlled by law, implement laws.

Motivation State the motivation of the stakeholder for having any reason of considering the cloud for its work or the motivation for having any kind of relation to stakeholders of the direct or indirect environment, e.g. protect privacy of citizens or implement concrete laws of an economic community.

Compliance and Privacy Identify relevant compliance and privacy laws and regulations for the cloud scenario, e.g. BDSG and KonTraG.

B. Instantiation of Cloud System Analysis Pattern

We now generally explain the process of instantiating our cloud system analysis pattern. Figure 3 shows an instance of our cloud system analysis pattern regarding the online banking service example.

1) Instantiate the direct system environment
   a) State the instantiations of the cloud stakeholders of the direct system environment, e.g. which company is the cloud provider.
   b) Moreover, the stakeholders defined by the cloud system analysis pattern can be complemented by further stakeholders.
   c) For each direct stakeholder instantiate the direct stakeholder template.

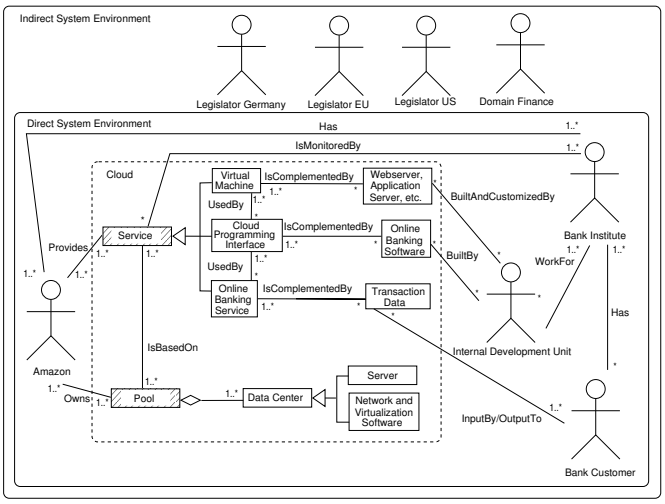

Figure 3. Concrete Cloud Computing System for Online Banking Service

In our example in Fig. 3, we assume that the cloud provider is Amazon, the cloud customer is the Bank Institute, the end customers are Bank Customers, and the cloud developer is the Internal Development Unit of the Bank Institute.

2) Instantiate the cloud
   a) Provide a functional description of the software offered by the cloud. Define the cloud layer the software is located in, the in- and output of the service(s), and the connections to the stakeholders of the direct system environment.
   b) The Data might be analysed more precisely using, e.g. class diagrams. This helps to apply asset identification and analysis techniques in later development phases.
   c) Provide the geographical location(s) of the cloud.
   d) State the deployment scenario of the cloud (private, public, hybrid).
   e) State the technical implementation behind the system, e.g. the required applications in the cloud software stack to provide an SaaS offer.

   In our example in Fig. 3, we consider the Online Banking Service as an SaaS offer, and the data is instantiated with Transaction Data. The cloud of the provider Amazon is public, and the data centres are located in Germany as well as in the US.
3) Instantiate the indirect system environment
   a) Determine the relevant domains (e.g. finance, medical, insurance) for the cloud scenario by considering the outsourced processes of the cloud customer and select the relevant legislators (e.g. Germany, US). Relevant are legislators or jurisdictions, where the resources are located, i.e. where the data is physically stored and processed, and where users, providers and

cloud customers are based.

b) In addition to the indirect stakeholders covered by the cloud system analysis pattern, further indirect stakeholders can be added.

c) For each indirect stakeholder instantiate the indirect stakeholder template.

In our example in Fig. 3, the domain is the Domain Finance, and the relevant legislators are Germany, EU, and US (since the data centres of Amazon are located in Germany as well as in the US).

The cardinalities contained in the pattern can be instantiated in a restricting way only. When instantiating the cloud system analysis pattern, one also fills in the corresponding templates. As examples, we present the following two stakeholder template instances:

Name Legislator Germany

Description The Legislator Germany represents all German laws relevant for this cloud scenario.

Motivation The German laws try to control the risks of companies (Amazon and Bank Institute) and to protect the privacy of the Bank Customers by regulating disclosure of personal data.

Relations to other stakeholders Controlled by law: The laws have to be obeyed by all stakeholders of the Direct System Environment.

Compliance and Privacy The following regulations might be considered:

- Privacy protection: e.g. BDSG
- Risk management: e.g. AktG

Name Bank Customer

Description The Bank Customer uses the online banking service of the Bank Institute.

Motivation The Bank Customer wants cheap and secure financial transactions via the bank's cloud computing offer.

Relations to the cloud InputBy/OutputTo: InputBy *financial data, data related to a person* (required for billing of the Bank Institute and maintenance of the cloud)

Relations to other stakeholders Has: Bank Institute as SaaS provider

Assets Financial data, data related to the person

Compliance and Privacy The following regulations might be considered:

- Privacy protection: BDSG Section 3, Section 4, Section 9, Section 11
- Risk management: AktG Section 91, Section 93

IV. Pattern-Based Support of ISO 2700x

In Sect. IV-A, we describe an approach, how our instantiated cloud system analysis pattern and the corresponding stakeholder templates can support the context establishment step of the information security risk management process in ISO 27005, illustrated in Fig. 1. Then, in Sect. IV-B we present the support for the asset identification, which is part of the risk identification activity.

A. Context Establishment

One sub step of the context establishment, described in Clause 7.3, is the definition of the *scope and boundaries* of information security risk management. As mentioned in Sect. I, the input for this step, which is the initial input for the whole information security risk management process, is left much open and is imprecise. Our cloud system analysis pattern supports this step by systematically eliciting the necessary input. For defining the scope and boundaries, the ISO recommends to consider the following information [1, Clause 7.3]:

1) The organisation's strategic business objectives, strategies and policies
2) Legal, regulatory and contractual requirements applicable to the organisation
3) Information assets
4) Locations of the organisation and their geographical characteristics
5) Expectation of stakeholders
6) Interfaces (i.e. information exchange with the environment)

In the following we describe how parts of this information can be systematically collected for the information security risk management of a cloud scenario by our cloud analysis pattern.

The Motivation in the direct stakeholder template instances can help to elevate business objectives, requested at 1). In Sect. III-B we showed an example instance for the Bank Customer. Even those motivations of related stakeholders help deriving business goals for the Bank Institute, representing the organisation applying ISO 27000 series for information security. Thus, a business goal of the Bank Institute is offering a secure online banking service and using therefore the cloud to reduce costs. For bullet point 2), we currently develop a law pattern to identify laws relevant for cloud scenarios. We focus in Sect. IV-B on bullet point 3), information asset, because assets are faced in ISO 27005 more detailed in the later step of asset identification, documented in Clause 8.2.1.2. For the locations and the geographical characteristics, the information about Data Centers in our pattern can be used. The instantiation happened in 2c of our stakeholder template instantiation process. According to our online banking example, Germany and the US are relevant locations to be considered for the information security risk management.

The needed expectations of stakeholders at 5) can be interpreted as collecting security requirements of the different stakeholders involved. Requirements engineering methods, as treated in [7], often start with an contextual analysis of

the environment, that can be offered by our cloud system analysis pattern instance.

For identifying the interfaces at bullet point 6), the associations in Fig. 3 can be used as indicator. They represent the information exchange between the stakeholders, i.e. the environment, and the cloud. Thus, there must be interfaces to allow this exchange on a technical level. In our online banking example interfaces exist for the Bank Customer to exchange data with the cloud, for the Internal Development Unit to deploy the software into the PaaS layer of the cloud, for the Bank Institute to monitor ongoing customer activities in the cloud as well as putting data into the cloud and for the Cloud Provider to control for example resources to generate billing data or to maintain the cloud.

The context establishment contains further sub step as "setting the basic criteria necessary for information security risk management" [1, Clause 7.2] and "establishing an appropriate organisation operating" it [1, Clause 7.4]. Those steps are for example about defining *risk acceptance criteria*, i.e. defining scales and thresholds for levels of risk acceptance or setting up roles and responsibilities of the organisation to manage the risk process. Our pattern does not support providing relevant information for these steps.

B. Asset Identification

In Clause 8.2.1.2, a sub part of the risk analysis step, the ISO standard requires the identification of assets within the established scope of the organisation at an appropriate level of detail. The Annex B extends the given information for the identification of assets and distinguishes between *primary assets* and *supporting assets*. Primary assets are *business processes*, *activities* and *information*. Supporting assets are *hardware*, *software*, *network*, *personnel*, *site* or *organization's structure*. The Annex B.1.2 offers a concrete list of examples for every supporting asset. The input for the identification of assets are the scope and boundaries identified in the context establishment activity.

The cloud system analysis pattern instance in Fig. 3 helps identifying the primary and supporting assets by considering the instantiated boxes and the associations between the direct stakeholders and the cloud. The associations indicate the flow of information into and out of the cloud and therefore helps to analyse the information assets processed and stored in the cloud. Furthermore, the associations help to find out about the *asset owner*, as the standard requires. "The asset owner is often the most suitable person to determine the asset's value" and is used for asset valuation in Clause 8.2.2.2.

For instance, Transaction Data is related to the Bank Customer in Fig. 3. Thus, Transaction Data, that can be later refined to more concrete assets like account number or account balance, can be identified as a primary information asset. The owner of that asset is the Bank Customer.

The ISO standard states, that the primary asset information comprises *vital information*, *personal information*, *strategic information* and *high-cost information*. Vital information are relevant for running the organisation's business, personal information comprises personal data or privacy relevant data, strategic information are required for achieving business goals and high-cost information are information whose gathering or processing require a long time or high acquisition cost. For example our pattern helps categorising Transaction Data as personal information due to the relation to the Bank Customer. Here, privacy related data, e.g. account balance, are exchanged with the cloud. Further, billing data can be seen as vital information for the Cloud Provider to run its business.

The cloud in Fig. 3, surrounded by the dashed line, structures the cloud system and the instantiated boxes represent supporting assets. For example different refinements of the supporting asset software can be found: Virtualisation Software as well as the Online Banking Software. The latter is deployed into the cloud by the Internal Development Unit, who could be wrongly determined as the asset owner. Using the associations in our pattern it can be analysed, that the Internal Development Unit WorkFor the Bank Institute, who is therefore a more appropriate owner of the Online Banking Software, because it has contracted the software.

"The personnel type consists of all the groups of people involved in the information system." as for example *users*, *developers* or *decision maker*. The stakeholder in the Direct System Environment as well as the Indirect System Environment support the refinement of this supporting asset in the standard. "The site type comprises all the places containing the scope or part of the scope" and can be seen related to the location and geographical information of Clause 7.3 mentioned in Sect. IV-A. Here, also the location of the Data Centers can help to identify relevant information. In the example list of Annex B.1.2. one refinement of the location is *external environment*. "This concerns all locations in which the organisation's means of security cannot be applied". That could mean for our example, that personal data processed or stored in data centers of the US, do not comply to German privacy laws and therefore this has to be documented here.

The organisation's structure are for example *subcontractors* of the organisation. Here, the Direct Stakeholder Environment could help identifying them. The Cloud Provider as well as the Internal Development Unit can be documented here.

Our pattern does not cover identifying all types of assets completely yet. For example there have to be done research on helping to identify business process and activity assets.

V. Envisaged Tool Support

In the following, we outline an *automated approach*, that provides digital patterns and templates for the context establishment and asset identification in accordance with the

ISO 2700x standards. A *modular user interface* will support users in following the supported parts of the context establishment. It provides *wizards* for instantiating the pattern and the templates. *Graphical modelling elements* will represent different patterns and types of data. In the following step, users identify assets from the generated patterns and templates. The tool will offer a *database* for storing instantiated patterns. This reduces the workload for instantiating similar systems. It also enables the tool to learn over time and enrich the wizards. The planned *recommender* will contain instantiated patterns and templates, and identified assets in their context. Therefore, the recommender can advise to look for specific assets or remind the user that an asset might be missing.

VI. Related Work

Mayer et al. [8] propose a security requirements engineering process that consists of the following four steps: Context analysis and asset identification, security goal determination, refinement of these goals to security requirements, and countermeasures selection. Both of the latter two steps are based on a risk analysis approach named model-based ISSRM.

Schmidt [7] presents a threat and risk-driven methodology to security requirements engineering. His approach shows threat and risk models derived from the environment of a secure information system and is therefore a complementation of our approach.

Haley et al. [9] propose a framework which unifies functional requirements from requirements engineering and assets as well as threats from security engineering. The focus of this work is the transformation of assets and threats into constraints of functional requirements.

Fenz et al. [10] introduce an ontology-based framework for preparing ISO 27001 audits. They provide a rule-based engine which uses a security-ontology to determine if security requirements of a company are fulfilled.

VII. Conclusion and Future Work

We presented a *pattern-based support for context establishment and asset identification* for the ISO 2700x standards in the field of cloud computing. This approach serves as a proof-of-concept that security standards can largely benefit from patterns. Our approach comprises the following main benefits:

- Systematic pattern-based identification of assets and context establishment for clouds
- Ease the burden of the initial steps of implementing the ISO 2700x standards
- Improve the outcome of a ISO 2700x implementations by perfecting the initial steps context establishment and asset identification

The work presented here will be extended to support further parts of implementing the ISO 2700x standards. We plan to provide patterns and templates for other steps of the standard, e.g. considering systematically business processes and activities. In addition, we intend to develop a general method to support the early steps of the standard, and apply it for instance as validation to the BSI Standard 100-2.

Acknowledgment

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).

References

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

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," EECS Department, University of California, Berkeley, Tech. Rep., 2009.

[3] P. Mell and T. Grance, "The NIST definition of cloud computing," Working Paper of the National Institute of Standards and Technology (NIST), 2009.

[4] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: Towards a cloud definition," *Special Interest Group on Data Communication (SIGCOMM) Computer Communication Review*, vol. 39, no. 1, pp. 50–55, 2008.

[5] R. Buyya, R. Ranjan, and R. N. Calheiros, "Modeling and simulation of scalable cloud computing environments and the cloudsim toolkit: Challenges and opportunities," in *Proceedings of the International Conference von High Performance Computing and Simulation (HPCS)*. IEEE Computer Society, 2009.

[6] BSI, "IT-Grundschutz-Vorgehensweise," Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI Standard 100-2, 2008.

[7] H. Schmidt, "Threat- and risk-analysis during early security requirements engineering," in *Proceedings of the International Conference on Availability, Reliability and Security (ARES)*. IEEE Computer Society, 2010, pp. 188–195.

[8] N. Mayer, A. Rifaut, and E. Dubois, "Towards a risk-based security requirements engineering framework," in *Proceedings of the International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ)*, 2005.

[9] C. B. Haley, J. D. Moffett, R. Laney, and B. Nuseibeh, "A framework for security requirements engineering," in *Proceedings of the International Workshop on Software Engineering for Secure Systems (SESS)*. ACM, 2006, pp. 35–42.

[10] S. Fenz, G. Goluch, A. Ekelhart, B. Riedl, and E. Weippl, "Information security fortification by ontological mapping of the ISO/IEC 27001 standard," in *Proceedings of the International Symposium on Dependable Computing*. IEEE Computer Society, 2007, pp. 381–388.