Pattern-Based and ISO 27001 Compliant Risk Analysis for Cloud Systems

Azadeh Alebrahim, Denis Hatebur
Paluno – The Ruhr Institute for Software Technology
University of Duisburg-Essen, Germany
Email:firstname.lastname@paluno.uni-due.de

Ludger Goeke
ITESYS GmbH
Dortmund, Germany
Email: L.Goeke@itesys.de

***Abstract*—For accepting clouds and using cloud services by companies, security plays a decisive role. For cloud providers, one way to obtain customers' confidence is to establish security mechanisms when using clouds. The ISO 27001 standard provides general concepts for establishing information security in an organization. Risk analysis is an essential part in the ISO 27001 standard for achieving information security. This standard, however, contains ambiguous descriptions. In addition, it does not stipulate any method to identify assets, threats, and vulnerabilities. In this paper, we present a structured and pattern-based method to conduct risk analysis for cloud computing systems. It is tailored to SMEs. Our method addresses the requirements of the ISO 27001. We make use of the cloud system analysis pattern, security requirement patterns, threat patterns, and control patterns for conducting the risk analysis. The method is illustrated by a cloud logistics application example.**

I. Introduction

Cloud computing represents a technology as well as a business model [2]. *National Institute of Standards and Technology (NIST)* defines following properties for the cloud computing systems [18]: the cloud customer can require resources of the cloud provider such as storage, processing, memory, network bandwidth, and virtual machines over *broad network access* and *on-demand* and pays only for the used capabilities. Using cloud computing services is thus an economic way of acquiring IT-resources. The dynamic acquisition and scalability, yet paying only what was used, makes cloud computing an interesting alternative for a large amount of potential customers.

To benefit from cloud computing and the advantages it offers, obstacles regarding the usage of clouds should be cleared. For accepting clouds and using cloud services by companies, security plays a decisive role[1]. For cloud providers, one way to obtain customers' confidence is to establish security mechanisms when using clouds by certifying their cloud computing systems. The ISO 27001 standard [13] provides general concepts for establishing information security risk management in an organization. The Annex A of the ISO 27001 standard describes the normative controls of the standard. Risk analysis provides a foundation to the security of each organization. Hence, it is an essential part of the ISO 27001 standard for achieving information security. This standard does not stipulate any method for performing risk analysis. To identify assets, threats, and vulnerabilities as essential building blocks to security risk assessment, the companies offering cloud services need structured and comprehensible methods.

In this paper, we present a structured and pattern-based method to conduct risk analysis for cloud computing systems. Our method is based on [3]. In contrast to [3], we make use of threat patterns and control patterns for the risk assessment and tailor the method to small and medium enterprises (SMEs). Our method addresses the requirements of the ISO 27001 and uses the information provided by the ISO 27005 standard. Our method is compliant to the ISO 27001: 2005 and its first revision the ISO 27001: 2013 standard [16]. The ISO 27001: 2013 standard differs from the ISO 27001: 2005 standard in its structure and the abstraction level of specifying security requirements. The requirements specified in the ISO 27001: 2013 are more generic leading to more freedom regarding the way of implementing them. For example in the ISO 27001: 2013 standard, the identification of assets, threats, and vulnerabilities must not be performed before the identification of security risks, as it is the case in the ISO 27001: 2005 standard[2]. This revision however causes more ambiguity for establishing an information security management system (ISMS) according to the ISO 27001: 2013 standard. Hence, our method follows the requirements of the ISO 27001: 2005 standard. As this version demands more specific requirements for establishing an ISMS than the ISO 27001: 2013 standard, our method fulfills the requirements of the ISO 27001: 2013 standard as well.

We make use of the Cloud System Analysis Pattern (CSAP) [7] for defining the scope and boundaries of the ISMS, Threat Patterns (TP) for identifying threats, Security Requirement Patterns (SRP) [4] for eliciting security requirements, and Control Patterns (CP) based on the ISO 27002 standard [15] and the CSA Cloud Control Matrix (CCM)[3] for fulfilling identified security requirements in order to treat the unacceptable risks. We embed the patterns that we apply in a method that guides the companies through the process of risk analysis in a structured manner.

We apply our pattern-based method for performing risk analysis according to the ISO 27001 standard for an IaaS for the cloud system of our industry partner LANFER SYSTEMHAUS [4] to show the applicability of our approach. The LANFER SYSTEMHAUS provides infrastructure for logistic cloud services. It is based on virtual machines that provide a specific cloud platform.

This paper is organized as follows. We briefly present the ClouDAT framework, the CSAP, and the SRPs as basics

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

[2] http://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf

[3] https://cloudsecurityalliance.org/research/ccm/

[4] http://www.lanfer-systemhaus.de

of our proposed method in Sect. II. Our pattern-based risk analysis method and its application to our running example is introduced in Sect. III. Related work is discussed in Sect. IV. We conclude the paper in Sect. V.

II. Background

This section outlines the basic concepts of our method.

A. The ClouDAT Framework

The ClouDAT framework is a result of the ClouDAT project[5]. The ClouDAT framework will be available as open-source for all interested parties. This allows interested parties to try out and use the framework free of charge. The goal of this framework is to provide a means for SMEs to establish a cloud-specific ISMS compliant to the ISO 27001 [13] standard. An ISMS is a process that ensures the security of an organization or parts thereof. Currently, the framework includes:

- A structural meta-model of a cloud and a corresponding context-pattern and templates to elicit all relevant information of a cloud scenario [7].
- A simple method that describes how to conduct a security analysis and to establish a cloud-specific ISMS [3].
- Tool-support for eliciting and analyzing the required informationfor an ISO 27001 certification [5].
- A catalog for Security Requirement Patterns [5].
- A catalog for Threat Patterns.
- A catalog for Vulnerabilities.
- A catalog for Control Patterns.
- A mapping of threat patterns to Vulnerabilities.
- A mapping of Security Requirement Patterns to Control Patterns.

B. The Cloud System Analysis Pattern

In this section, we briefly introduce our Cloud System Analysis Pattern (CSAP) [7]. It provides the elements and structure to describe a cloud computing system. Furthermore, it models relations between, e.g., stakeholders and cloud elements. Due to the lack of space, we do not show the CSAP. A cloud scenario can be represented by instantiating the different elements in the pattern. The instantiation starts with identifying the potential cloud customers in the CSAP that represents the required cloud services for supporting their relevant business case. Then, we instantiate the cloud, which consists of different types of cloud elements. Cloud elements represent the physical cloud resources and the cloud services that provide these cloud resources to the cloud customers. The resources of cloud customers that are executed in the cloud are also represented by cloud elements. Cloud resources represent the required hardware and software supplied by cloud providers. These resources are provided via cloud services. The modeling of the cloud resources enables statements about the security of a cloud service. Assets represent anything that has a value [13]. Assets can be, for example, different occurrences of information or physical objects. An asset can be information, cloud data, documentation, and physical object. Cloud elements can have relations to each other. Furthermore, assets can have relations with the cloud elements that process, produce and/or store assets.

[5]http://www.cloudat.de

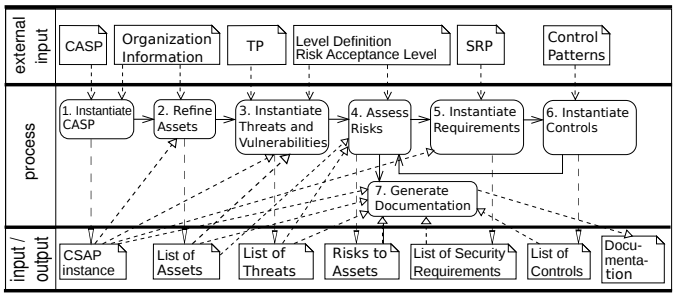

Fig. 1. Overview of the pattern-based risk analysis method

C. The Security Requirement Patterns

In this step, we describe our security requirement patterns (SRP) [4]. The resulting security requirements are related to elements in the CSAP instance. According to [10], a security requirement is typically a confidentiality, integrity or availability requirement. In our method, these kinds of requirements concern the different elements in a CSAP instance. A security requirement pattern contains always *fixed text passages* that represent the meaning of the security requirement pattern and *variable text passages*. Variable text passages have the following structure:

- [ ]: Opening and closing squared brackets mark the beginning and end of a variable text passage, respectively.
- *instance type of CSAP element*: In this case, a variable text passage references certain elements in the corresponding CSAP. They consider all elements whose instance types correspond to the keyword in the variable text passage.

During the instantiation of a security requirement pattern, the potential cloud customer can select the elements for which the surrounded fixed text applies.

Example for an SRP: "Confidentiality of *personal data* of [cloud customer, end customer] shall be achieved."
To instantiate the security requirement pattern, the CSAP instance representations of *cloud customer* and *end customer* shall be inserted into the variable text passage.

III. Pattern-based Risk Analysis

A. Phase 1: Instantiate CSAP

The aim of this phase is defining the scope and boundaries of the information security management system. The scope has to be specified before the start of the risk analysis. In the context of the ClouDAT framework the scope is specified by instantiating the CSAP (see Sect. II-B).

B. Phase 2: Refine Assets

This phase corresponds to Sect. 4.2.1 d 1 of ISO 27001 standard. The goal of this phase is the identification of assets that are relevant for the risk analysis. An asset represents "anything that has a value to the organization" according to ISO 27001 standard [13]. For the identified assets we conduct the risk analysis. We consider assets that are contained in the scope for the ISMS.

We make use of an asset template, in which we capture all the information we collect in steps 1 and 2 of this phase. The asset template including values obtained from steps 1 and 2 is shown in Tab I. In the following, we describe each step in detail.

TABLE I
INSTANTIATED ASSET TEMPLATE

Asset label	Asset	Owner	Location	Cloud element instance type	Relationship
AS-DA-001	Controlling data	Business project handling	Office 2	Data	AS-PS-002
AS-SW-023	Microsoft exchange	Normal Operation	Datacenter 1	Software	AS-DA-020
AS-DA-044	Monitoring message	Normal Operation	Datacenter 1	Data	AS-DA-042
AS-DA-048	Backup	Normal operation	Datacenter 1	Data	AS-HW-046
AS-HW-104	VM host server	Datacenter	Datacenter 1	Hardware	-

TABLE II
AN EXCERPT OF IDENTIFIED ASSETS, RELATED CLOUD ELEMENTS, AND EXISTING CONTROLS

Asset label	Existing control (C)	Existing control (I)	Existing control (A)
AS-DA-001	Access control, server in secured area	Access control, server in secured area	daily Backups, RAID system
AS-SW-023	server in secured area	server in secured area	RAID system, CD to install available
AS-DA-044	only send to limited number of employees	no existing control	send to more than one employee
AS-DA-048	stores in secured area with restricted access of few employees	stores in secured area with restricted access of few employees	Representatives
AS-HW-104	no existing control	server in secured area	redundant server in secured area

Step 1: Refine assets and their location: The aim of this step is to refine the assets for which we conduct the risk analysis. The high-level assets are directly identified by instantiating the CSAP. Thus, as input for this step, we take the instantiated CSAP, business characteristics of the organization, the organization processes, and the location of the organization into account.

The CSAP instance that specifies the relevant ISMS scope is the starting point for our asset refinement. All cloud elements that are contained in the relevant CSAP instance are assets. These assets are very abstract. For this reason, they have to be refined into more fine-grained assets. This refinement is repeated till we get assets that have an appropriate abstraction level for the risk analysis.

For this phase, we considered documents provided to us from the LANFER SYSTEMHAUS about the organization, work instructions, and organigrams to identify assets, related locations, and responsibilities. In additions, we visited the data center of the LANFER SYSTEMHAUS to identify further assets that we could not identify only by considering the documents. Altogether, we identified 105 assets.

This step also considers the identification of the location that an asset belongs to.

Step 2: Assign responsibilities and relationships: Identifying the responsibilities of assets and relating them to already identified assets are essential constituents of asset identification. To this end, we identify the owners of assets and add them to the asset template.

During the refinement of assets, we have to identify the relationships, which might exist between assets. We will make use of such information for risk assessment in phase 4.

In addition, we relate the identified assets to the elements of the instantiated CSAP. Table I represents the instantiation of the asset template as a result of steps 1 and 2 for our example. As a result, we obtain an instantiated Asset Template that contains the information about the identified assets regarding label, name, owner, location, relations between assets, and type of cloud element.

C. Phase 3: Instantiate Threats and Vulnerabilities

The threat analysis is applied to all assets that have been identified during phase 2. During an ordinary threat analysis it is examined if an asset is menaced by threats. Furthermore, it is analyzed if an asset has vulnerabilities that could be exploited by a threat.

To support the threat analysis our method provides *Threat Patterns (TP)*, which enable the reuse of knowledge regarding threats that has been gained during a threat analysis. We provide a catalog of predefined TP which were created based on the state of the art works (e.g. [8], [12], [9]). Among others, we have considered the list of seven threats released by the Cloud Security Alliance (CSA) [8], an industrial consortium that investigated practical security issues with clouds. We use this particular list of cloud threats, because it summarizes the experience in the field of cloud computing from the point of view of a large industrial consortium. Examples for such cloud threats are *Insecure Interfaces and APIs* and *Data Loss or Leakage*.

Our predefined TP facilitate and accelerate the threat analysis, as the users do not have to search for threats and assign the found threats to the relevant assets. Furthermore, the danger is reduced that an essential threat is not considered.

In our method, the structure of TP is defined by a UML meta-model. A TP specifies a potential threat to a type of asset. In a TP, this threat-asset-relation is represented by generic placeholders in form of the relevant asset type. During the instantiation of a TP these placeholders are substituted by the names of relevant assets of the corresponding type. An example for a TP is "Unavailability of [*cloud element*] for [*all end customer and cloud customer*]". Similar to SRP, a TP contains *fixed text passages* that represent the meaning of the threat pattern and *variable text passages* as placeholders that reference certain elements in the CSAP. To instantiate the threat pattern, the CSAP instance representations of *cloud element* and *all end customer and cloud customer* shall be inserted into the variable text passage.

It should be mentioned that our catalog of TP serves as a broad starting point for the threat analysis but does not claim to be complete. Each application of the catalog can extend the set of TP, if necessary. Such an extension of the catalog is possible, as the structure of TP is specified by a UML meta-model. According to this, the knowledge collected during a threat analysis can be recorded in a re-usable form.

Step 1: Identify threats and vulnerabilities: This step considers the identification of threats and vulnerabilities. It corresponds to Sections 4.2.1 d 2 and 4.2.1 d 3 of the ISO 27001 standard. We identify the threats for different types of previous refined assets by instantiating the TP relevant for the assets. The instantiation is achieved by substituting the appropriate placeholder in the considered TP by the name of a menaced asset. In addition to the TP, we provide a catalog of vulnerabilities that can be used as a basis to identify relevant vulnerabilities. It is subdivided into the categories confidentiality, integrity, and availability. We related TP to possible vulnerabilities by providing a mapping among them. For each instantiated threat, one has to check whether there exist vulnerabilities that can be exploited by the instantiated threat.

If this is the case, we have to select relevant vulnerabilities among the set of possible vulnerabilities related to each TP. Otherwise, the instantiated threat does not hit a vulnerability. Hence, it does not need to be considered in the further risk analysis. Note that we have to consider existing controls when identifying vulnerabilities. Table II depicts the list of existing controls for each identified asset.

Step 2: Define threat and vulnerability levels: In this step, we determine the likelihood of each threat and define the level of vulnerabilities. The likelihood scale of threats can be classified in *LOW* and *HIGH* as default values. A *LOW* threat likelihood represents *minor interest of attackers*, whereas a *HIGH* threat likelihood shows an *interest of attackers to threaten the asset*.

We define three levels of vulnerabilities, namely *L*, which represents *almost no vulnerability because all identified threats are addressed by controls*, *M*, which represents that a *basic protection is given*, and *H*, which represents that *threats are not addressed by controls*.

The likelihood of threats and the levels of vulnerability will be used later on (in Phase 4) to determine the likelihood for potentially occurring security failures. We show in Table III the results of identifying threats and vulnerabilities for our example.

D. Phase 4: Assess Risks

Risk management is mentioned in sections 4.2.1 e 1 - 4.2.1 e 4 of the ISO 27001 standard. In the approach, risk is used to assess if an asset requires further risk treatment or not. Before the risk analysis starts, the risk approach has to be specified. The risk approach contains the selection of an adequate methodology for the risk assessment that produces comparable and reproducible results. Furthermore, the level for accepting risks has to be defined. This risk acceptance level has to be committed by the management.

Step 1: Assess business impact: This step is concerned with assessing the business impact. It corresponds to Sections 4.2.1 d 4 and 4.2.1 e 1 of the ISO 27001 standard. Business impacts represent consequences that implicate the loss of security goals (e.g confidentiality, integrity, or availability) of an asset in course of a security incident. A business impact has to be assessed by an impact value.

In the following, the assessment of the impact value is described. The assessment of the business impact considers only those assets with vulnerabilities that are menaced by the identified threats. Therefore, as input for assessing the business impact, we need the list of assets. The business impact is expressed in form of impact criteria that is relevant for the organization. These criteria can represent monetary, technical and/or human criteria. The measurement of the determined business impact shall be suitable for the organization. We define impact values and the related impact criteria as represented in Table IV. Then, we assess the business impact for each identified asset according to these criteria.

Step 2: Determine security failures: Threats to and vulnerabilities of assets have been analyzed in phase 3 of our method. In this step, which corresponds to Sect. 4.2.1 e 2 of the ISO 27001 standard, we determine the likelihood of potential security failures for all threatened assets that have been identified in phase 3. The security failure scale has to be defined using the threat likelihood scale and the vulnerability level scale. Our default security failure values are given in Table V.

TABLE IV
IMPACT VALUE SCALE (CONSEQUENCE SCALE)

Impact value	Description
1	no consequence if asset is successfully threaten
2	consequence can be easily handled
3	to handle consequences moderate effort is necessary
4	to handle consequences high effort is necessary
5	company survival uncertain if asset is successfully threaten

TABLE V
SECURITY FAILURE LIKELIHOOD SCALE (VL: VULNERABILITY LEVEL, TL: THREAT LIKELIHOOD)

Security failure	(VL, TL)	Description
1	(L,LOW)	Almost no vulnerability because all identified threats are addressed by controls and attackers have only minor interest
2	(M,LOW)	Basic protection is given and attackers have only minor interest
3	(H,LOW) or (L,HIGH)	Possible threats are not addressed by controls and attackers have only minor interest/ Almost no vulnerability because all identified threats are addressed by controls and attackers have an interest to threaten asset
4	(M,HIGH)	Basic protection is given and attackers have an interest to threaten asset
5	(H,HIGH)	Possible threats are not addressed by controls and attackers have an interest to threaten asset

Step 3: Estimate risk levels: In this step, the level of risks for all affected assets has to be estimated. It corresponds to Sect. 4.2.1 e 3 of the ISO 27001 standard. We estimate the levels of risk by multiplying the likelihoods for security failures and values of business impacts that have been determined in the previous steps. Using a security risk evaluation matrix as in the ISO 27005 standard [14], we derived a risk acceptance level of 8.

Table VI represents the results of steps 1 (business impact), 2 (security failure), and 3 (risk level) for our example.

Step 4: Verify the risk level: After the estimation of the risk level, it has to be verified if the risk level corresponds to an acceptable risk level. The acceptable risk level in our example is 8. If the level of a risk does not correspond the acceptable risk level, this risk has to be treated. This step corresponds to Sect. 4.2.1 e 4 of the ISO 27001 standard. For every risk that needs treatment the priority for the treatment is deduced by the risk level. The ISO 27001 specifies the following treatments: 1) applying appropriate controls, 2) accepting risks, 3) avoiding risks, and 4) transferring the associated business risks to other parties.

E. Phase 5: Instantiate Security Requirements

This phase considers all assets that have an unacceptable risk level that should be treated by selecting controls. Here, the selected controls shall decrease the risk level. The results of the risk level estimation for the above mentioned assets lead to security requirements for these assets. For creating these security requirements, our method uses Security Requirement

TABLE VI
BUSINESS IMPACT (B.I.), LIKELIHOODS FOR SECURITY FAILURES (S.F.), AND THE ESTIMATED RISK LEVEL (R.L.) FOR IDENTIFIED ASSETS

Asset label	B.I (C)	B.I (I)	B.I (A)	S.F. (C)	S.F. (I)	S.F. (A)	R.L. (C)	R.L. (I)	R.L. (A)
AS-DA-001	4	3	2	3	2	2	12	6	4
AS-SW-023	-	2	3	-	2	2	-	4	4
AS-DA-044	2	2	2	2	5	3	4	10	6
AS-DA-048	2	2	3	3	2	1	6	4	3
AS-HW-104	-	1	5	-	3	3	-	-	15

TABLE III
AN EXCERPT OF IDENTIFIED ASSETS, RELATED THREATS, AND VULNERABILITIES (C: CONFIDENTIALITY, I: INTEGRITY, A: AVAILABILITY)

Asset label	Threat (C)	Threat (I)	Threat (A)	Vulnerability
AS-DA-001	Disclosure of stored *controlling data* of *LANFER SYSTEMHAUS* by *an attacker*	Modification of *controlling data* by an attacker	Unavailability of *controlling data* for *LANFER SYSTEMHAUS*	e.g., gaining access to secured area (C,I,A)
AS-SW-023	-	Modification of *Microsoft Exchange* by *an attacker*	Unavailability of *Microsoft Exchange* for *LANFER SYSTEMHAUS*	e.g., impersonation as administrator and installing modified Exchange software (I)
AS-DA-044	Disclosure of communication between *virtual machine* and *employees*	Modification of communication between *virtual machine* and *employees* to modify *monitoring message*	Unavailability of communication between *virtual machine* and *employees*	e.g., network sniffing to read monitoring messages (C)
AS-DA-48	Disclosure of stored *backup* of *LANFER SYSTEMHAUS* by *an attacker*	Modification of *backup* by an attacker	Unavailability of *backup* for *LANFER SYSTEMHAUS*	e.g., responsible person and all representatives are not available when access to backup is necessary (A)
AS-HW-104	-	Modification of *VM host server* by an attacker	Unavailability of *VM host server* for *LANFER SYSTEMHAUS*	e.g., gaining access to secured area (I,A)

Patterns (SRP) [5]. These SRP follow the same principles like the already mentioned Threat Patterns. This means SRP contain placeholders that are substituted by the names of relevant assets of the corresponding instance type during the creation of SRP.

Our method provides a catalog of predefined SRP. Furthermore, we have specified a mapping between the predefined SRP and the Threat Patterns from phase 3. This means that Threat Patterns are linked to the SRP that are relevant for the assets, which are menaced by the described threat.

Security requirements are of importance, because they allow a statement if they are fulfilled or not. Hence, if all security requirements of a cloud scenario are fulfilled, we can state that the security level of a cloud system is sufficient. The creation of security requirements for an asset is simplified by instantiating the relevant security requirement patterns that are referenced by the appropriate Threat Patterns. For more information regarding SRP, we refer to our previous work [4].

Using the mapping between TP ans SRP, we select relevant SRP for the assets, which have an unacceptable risk level and instantiate them. Doing this, we obtain the following security requirements:

- SR 1 Preserve confidentiality of stored *controlling data* of the *LANFER SYSTEMHAUS* by preventing disclosure by *an attacker*.
- SR 2 The integrity of communication between *virtual machine* and *employees* shall be preserved.
- SR 3 Manipulation on *VM host server* that leads to the unavailability of it shall be prevented.
- SR 4 Sufficient physical protection shall be implemented (no windows in ground floor, access control for all entries with limited access for visitors, ...) to ensure availability regarding the *VM host server*.
- SR 5 Technical malfunctions of the *VM host server* shall not affect the availability of the *provided platform*.

F. Phase 6: Instantiate Controls

This step considers the treatment of risks by selecting appropriate controls. It corresponds to Sect. 4.2.1 f 1 of the ISO 27001 standard.

Security requirements have to be fulfilled by controls. The representation of controls in our method is specified by Control Patterns (CP). CP are referenced by their corresponding Security Requirement Pattern(s). We have created a catalog of predefined controls based on the ISO 27002 standard and the CSA CCM. The ISO 27002 standard provides a reference for selecting controls when implementing an ISMS based on the ISO 27001 standard. The structure of CP is also specified by a UML meta-model. Because of this the users can extend the CP catalog by their own Control Patterns.

We have also specified a mapping between our predefined SRP and predefined CP. This means that users have a preselection of CP that could be relevant for a certain security requirement. Using this mapping, users can instantiate each CP from this preselection which is relevant in the context of their cloud scenario. It is also possible that users define mappings between their own security requirements and controls. Using our provided mapping between SRP and CP, we select relevant CP listed as follows:

- C 1 To address the security requirement *SR 1*, we apply the controls of the ISO 27002:2013, e.g., equipment security (A.11.2), access control (A.9) including the controls according to our mapping, e.g. human resource security (A.7).
- C 2 to address the security requirement *SR 2*, cryptographic means for signatures were applied including the necessary measures from ISO 27002:2013 (A.10).
- C 3 To address the security requirement *SR 3*, we apply the same controls as for the security requirement *SR 1*. In addition, we apply the control A.11.1.
- C 4 Controls addressing the security requirement *SR 4* (e.g. A.11.1) were already in place (see Table II).
- C 5 To address the security requirement *SR 5*, controls for redundant servers (A.17.2) have to be applied.

After the selection of controls it has to be verified if the level of the risk has been reduced to an acceptable risk level. To this end, we have to go back to phase 4 of our method in order to adjust the risk assessment for that particular asset. This information is in turn used to check if the control already results in an acceptable risk level or if it has to be modified or another control should be introduced.

G. Phase 7: Generate Documentation

The final phase of our method is concerned with generating documentation. To this end, we require the CSAP instance as output of phase 1, the list of identified assets as output of phase 2, list of threats and corresponding vulnerabilities as output of phase 3, identified risks as output of phase 4, list of security requirements as output of phase 5, and finally, the list of controls to be implemented as output of phase 6. The resulting documentation is part of the ISMS documentation as *Statement of Applicability* to be required for the certification.

IV. RELATED WORK

CORAS [17] is a model-based approach with graphical representation for risk analysis. CORAS is based on ISO

31000. The five steps of ISO 31000 are *context establishment*, *risk identification*, *risk estimation*, *risk evaluation*, and *risk treatment*. CORAS does not take into account the ISO 27001 standard.

Beckers et al. [6] propose an extension to the CORAS risk analysis method. The extension provides support for the establishment of an ISO 27001 compliant Information Security Management System. ISMS-CORAS produces documentation that is required by the ISO 27001 standard. The focus of this extension is on risk management. In opposite to our risk analysis method, these two approaches [17], [6] do not consider threats specific to cloud systems, such as those released by the Cloud Security Alliance (CSA) [8].

Gandhi et al. [11] provide a method for structuring requirements as well as identifying and representing correlations between requirements. The method considers possible bypassing of requirements due cascading effects of failure. The method does not provide an approach for evaluating risks according to ISO 27005.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [1] is a risk-based information security assessment and planning approach. It consists of three phases for building asset-based threat profiles, identification of infrastructure vulnerabilities, and developing security strategy and mitigation plan. Similar to CORAS, OCTAVE does not support the ISO 27001 standard.

The Microsoft Security Risk Management Guide [19] provides support for organizations to security risk assessment. This approach does not support the fulfillment of the ISO 27001 standard, although there are some overlaps. In addition, it does not perform risk assessment, which is specific to cloud systems. Hence, the cloud-specific threats and resulting risks might not be identified by applying this approach.

V. Conclusion

We have presented a structured method for performing risk analysis according to the ISO 27001 standard. Our method relies upon patterns to describe the context and structure of a cloud computing system (CSAP), elicit the security requirements (SRP), identify threats (TP), and select controls (CP), which ease the effort for these activities. Our approach comprises the following main benefits:

- Systematic pattern-based identification of threats using TP and their relationship to CSAP elements which facilitates and accelerates the threat analysis
- Systematic pattern-based identification of security requirements to be fulfilled by appropriate controls using SRP and their relationship to TP
- Systematic pattern-based identification of controls using CP and their relationship to SRP

We started to perform the risk analysis for the SaaS and PaaS. We will evaluate this on a large scale. This involves the application of our method to the SaaS and PaaS for the cloud system of our industry partner LANFER SYSTEMHAUS. In addition, we will extend our risk analysis method with further phases to support the establishment of an ISMS according to the ISO 27001 standard. Currently, the ClouDAT framework tool contains a graphical representation of the CSAP for describing the cloud scenario, as well as instantiating the SRP. In the future, we want to extend the tool for supporting other types of patterns for performing risk analysis, such as TP and CP. In addition, we intend to enrich the tool with validation conditions to check the instantiation of the patterns. We strive for providing full tool support for our ClouDAT framework in order to support the ISO 27001 standard certification.

Acknowledgments

This research was partially supported by 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). We would like to thank Stefan Vorbau (LANFER SYSTEMHAUS) for providing required documents and supporting us by identification of assets.

References

[1] C. Alberts and A. Dorofee. *Managing Information Security Risks: The OCTAVE (SM) Approach*. Addison-Wesley Professional, 2002.

[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. Technical report, Berkeley, 2009.

[3] K. Beckers, I. Côté, S. Faßbender, M. Heisel, and S. Hofbauer. A pattern-based method for establishing a cloud-specific information security management system. *Requirements Engineering*, pages 1–53, 2013.

[4] K. Beckers, I. Côté, and L. Goeke. A Catalog of Security Requirements Patterns for the Domain of Cloud Computing Systems. In *Proc. 29th Symposium on Applied Computing*. ACM, 2014. Accepted for Publication.

[5] K. Beckers, I. Côté, L. Goeke, S. Güler, and M. Heisel. Structured pattern-based security requirements elicitation for clouds. In *Proc. of the 7th Int. Workshop on Secure Software Engineering (SecSE)*, pages 465–474. IEEE Computer Society, 2013.

[6] K. Beckers, M. Heisel, B. Solhaug, and K. Stølen. ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System. In *Engineering Secure Future Internet Services*, LNCS 8431, page 315344. Springer, 2014.

[7] K. Beckers, J.-C. Küster, S. Faßbender, and H. Schmidt. Pattern-based support for context establishment and asset identification of the ISO 27000 in the field of cloud computing. In *Proc. of the Int. Conf. on Availability, Reliability and Security (ARES)*, pages 327–333. IEEE Computer Society, 2011.

[8] CSA. Security guidance for critical areas of focus in cloud computing v3.0, 2011.

[9] European Network and Information Security Agency. Cloud computing - benefits, risks and recommendations for information security, 2009.

[10] B. Fabian, S. Gürses, M. Heisel, T. Santen, and H. Schmidt. A comparison of security requirements engineering methods. *Requirements Engineering – Special Issue on Security Requirements Engineering*, 15(1):7–40, 2010.

[11] R. A. Gandhi and S. W. Lee. Discovering multidimensional correlations among regulatory requirements to understand risk. *ACM Trans. Softw. Eng. Methodol.*, 20(4):16:1–16:37, Sept. 2011.

[12] J. Heiser and M. Nicolett. Assessing the security risks of cloud computing, June 2008.

[13] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001), 2005.

[14] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). Information technology - Security techniques - Information security risk management (ISO/IEC 27005), 2011.

[15] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). Information technology - Security techniques - Code of practice for information security controls (ISO/IEC 27002), 2013.

[16] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001), 2013.

[17] M. S. Lund, B. Solhaug, and K. Stølen. *Model-Driven Risk Analysis. The CORAS Approach*. Springer, 2010.

[18] P. Mell and T. Grance. The NIST definition of cloud computing. Special Publication 800-145 of the National Institute of Standards and Technology (NIST), 2011.

[19] Microsoft Corporation. The security risk management guide, 2006.