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

Azadeh Alebrahim, Denis Hatebur, Stephan Fassbender
Paluno – The Ruhr Institute for Software Technology, University of Duisburg-Essen, Germany
firstname.lastname@paluno.uni-due.de
Telephone: +49 203 3465
Oststraße 99, Building BB, 9th Floor
D-47057 Duisburg
Germany

Ludger Goeke[1], Isabelle Côté
ITESYS Inst. f. tech. Sys. GmbH
L.Goeke@itesys.de, I.Cote@itesys.de
Telephone +49 231 97 42 71 10
Emil-Figge-Straße 76
D-44227 Dortmund
Germany

Abstract

Security plays a major role when companies decide whether to move to the cloud and use cloud services. One way to obtain the confidence of the customers 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.

Keywords: risk analysis, patterns, ISO27001, cloud systems, ISMS

[1] Corresponding author

1 Introduction

Cloud computing represents a technology as well as a business model (Armbrust et al., 2009). The *National Institute of Standards and Technology (NIST)* defines the following properties for cloud computing systems (Mell & Grance, 2011): 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 number of potential customers.

To benefit from cloud computing and the advantages it offers, obstacles regarding the usage of clouds have to be cleared. Security plays a major role when companies decide whether to move to the cloud and use cloud services (IBM). For cloud providers, one way to obtain the confidence of the customers is to establish security mechanisms when using clouds by certifying their cloud computing systems. The ISO 27001 standard (ISO/IEC 27001, 2005) is applicable for this case. It provides general concepts for establishing information security risk management in an organization. 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 specific method for performing risk analysis. This is up to the discretion of the company. So, 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 Beckers et al. (2013a), we presented a method consisting of seven steps for setting up an information security management system which is tailored for clouds. In its fifth step, it uses CORAS (Lund et al., 2010) as one possible way of a risk management approach.
However, not all SMEs want or can use CORAS as their risk management approach. The reason is that CORAS is a diagram-based and more heavy-weight approach, which is not appropriate for SME's Cloud systems.
Most SMEs might already have their own approach or wish for a different one. As the PACTS method described in Beckers et al. (2013a) is modular in structure, it is possible to exchange methods used within the different steps.
Therefore, the PACTS method serves as a basis for the work presented here.
In this paper, however, we present a different structured and pattern-based method to conduct risk analysis for cloud computing systems, which means we provide a different method for Step 5of PACTS. The method proposed in this paper leans more towards the general requirements for conducting risk assessment presented in ISO 27005. It uses threat patterns and control patterns as well as information provided in ISO 27005 as means to fulfill risk management.
This approach has the following benefits:

- Maintaining catalogs of patterns for threats, security requirements,

vulnerabilities, and controls.
- Providing traceability links between different types of pattern catalogs.
- Use of patterns in nearly all phases of the risk assessment process.
- Automatic selection of possible patterns according to previously selected patterns.

Our method is compliant to the ISO 27001:2005 and its first revision, the ISO 27001:2013 standard (ISO/IEC 27001, 2013). 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 ISO 27001:2013, the identification of assets, threats, and vulnerabilities must not be performed before the identification of security risks, as it is the case in ISO 27001:2005 (BSI, 2014). This revision however causes more ambiguity for establishing an information security management system (ISMS) according to ISO 27001:2013. 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) (Beckers et al., 2011) for defining the scope and boundaries of the ISMS, Threat Patterns (TP) for identifying threats, Security Requirement Patterns (SRP) (Beckers et al., 2014a) for eliciting security requirements, and Control Patterns (CP) based on ISO 27002 (ISO/IEC 27002, 2013) and the CSA Cloud Control Matrix (CCM, 2014) for fulfilling identified security requirements in order to treat unacceptable risks. We embed the patterns that we apply in a method that guides 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 to the cloud system of our industrial partner LANFER SYSTEMHAUS (2014) to show the applicability of our approach. LANFER SYSTEMHAUS provides infrastructure for logistic cloud services. It is based on virtual machines that provide a specific cloud platform.

However, as we are currently not at liberty to disclose specific details of the cloud system, we provide rather generic examples throughout the case study.

This work is organized as follows. We briefly present the ClouDAT framework, the CSAP, and the SRPs as basics of our proposed method in Section 2 (Background). Our risk analysis method and its application to the running example are introduced in Section 3 (Pattern-Based Risk Analysis). We discuss our experiences regarding the application of our method in Section 4 (Lessons learned/Discussion). Our proposed tool support is described in Section 5 (Tool Support). Related work is discussed in Section 6 (Related Work). We conclude this work in Section 7 (Conclusion).

2 Background

This section outlines the basic concepts of our method.

2.1. *The ClouDAT Framework*

The ClouDAT framework is currently under development as part of the ClouDAT project (2014). 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 (ISO/IEC 27001, 2005) 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 (Beckers et al., 2011).
- A simple method that describes how to conduct a security analysis and to establish a cloud-specific ISMS (Beckers et al., 2013a).
- Tool-support for eliciting and analyzing the required information for an ISO 27001 certification (Beckers et al., 2013b).
- A catalog for Security Requirement Patterns (Beckers et al., 2013b).
- 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.

2.2. *The Cloud System Analysis Pattern*

In this section, we briefly introduce our Cloud System Analysis Pattern (CSAP) (Beckers et al., 2011). It provides the elements and structure to describe a cloud computing system. Furthermore, it models relations between, e.g., stakeholders and cloud elements (see Figure 1).

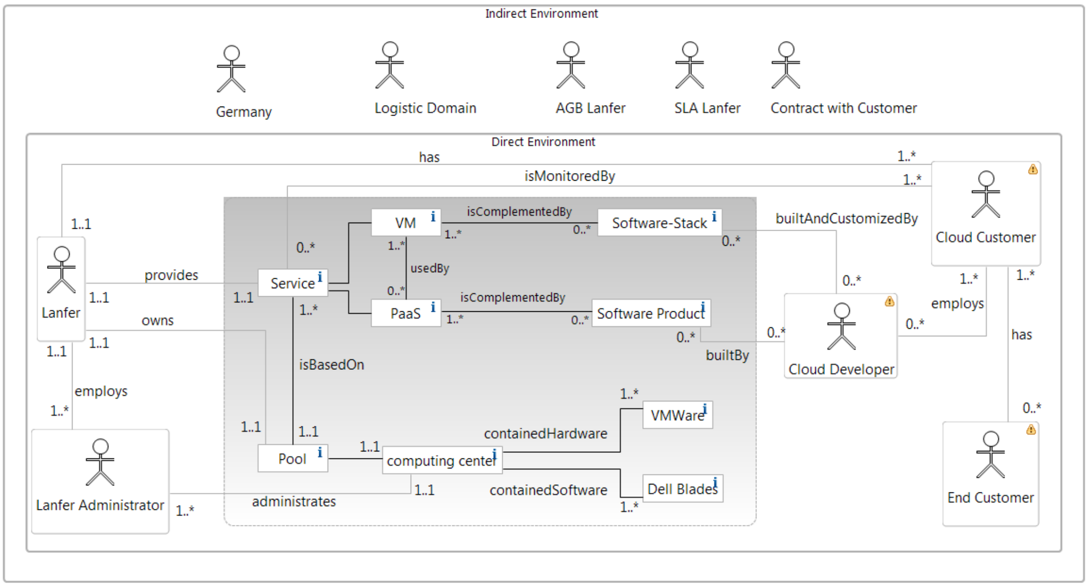


Figure 1 Cloud System Analysis Pattern instance

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. They require cloud services for supporting their relevant business case. The cloud provider offering these services has to be instantiated as well (see right-hand and left-hand side of Figure 1). It also takes entities into account that might not be directly linked to the cloud system at hand, but still need to be considered, such as legislators with their respective laws and regulations (see top of Figure 1). Then, we instantiate the cloud consisting of different types of cloud elements (see highlighted part in Figure 1). 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 (ISO/IEC 27001, 2005). 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.

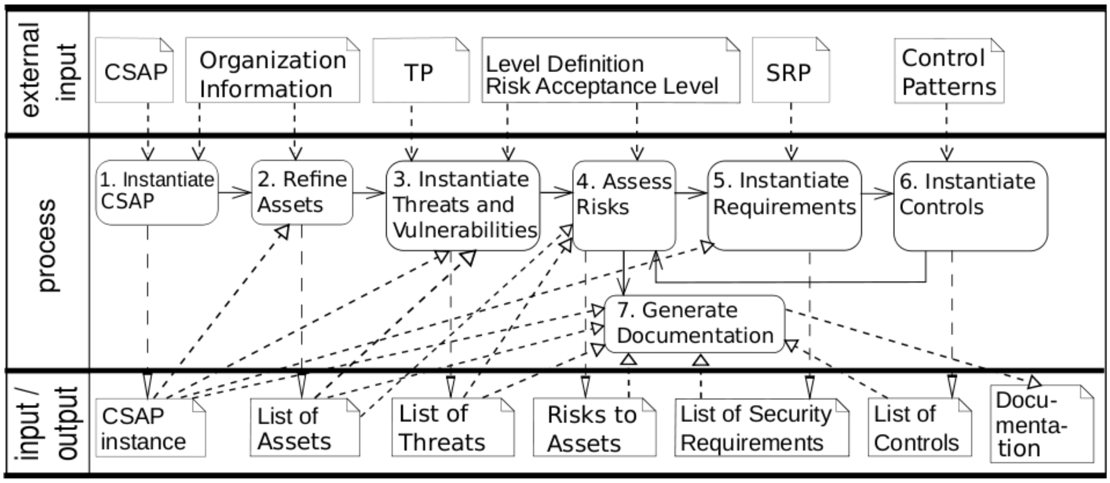


Figure 2 Overview of the pattern-based risk analysis method

2.3. The Security Requirement Patterns

In this phase, we describe our security requirement patterns (SRP) (Beckers et al., 2014a). The resulting security requirements are related to elements in the CSAP instance. According to (Fabian et al., 2010), 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(s) 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. An example for such an SRP is*:*

"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* or *end customer* shall be inserted into the variable text passage. This results in the following SRP instance:

"Confidentiality of *personal data* of LANFER SYSTEMHAUS shall be achieved."

3 Pattern-Based Risk Analysis

The following sections describe our pattern-based risk analysis method depicted in Figure 2 with its related input and output documents.

3.1. Phase 1: Instantiate CSAP

The aim of this phase is to define 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). For our case study, we considered documents from the LANFER SYSTEMHAUS to instantiate the CSAP (see Figure 1).

3.2. Phase 2: Refine Assets

This phase corresponds to Sect. 4.2.1 d 1 of ISO 27001:2005. The goal of this phase is to identify assets that are relevant for the risk analysis.

The goal is to refine the assets for which we conduct the risk analysis. The high-level assets are directly identified by instantiating the CSAP. Therefore, we take the instantiated CSAP, business characteristics of the organization, the organization processes, and the location of the organization as input for this step. 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 can be achieved by composition or specialization. This results in new assets to be considered.

Figure 3 shows an example of such a refinement applied to our case study. The 'computing center' is decomposed into 'Software' and 'Data In Computing Center'. These new assets are further decomposed. 'Microsoft Exchange' is an example for 'Software' and 'Controlling Data', 'Monitoring Message', and 'Backup' refine 'Data In Computing Center', respectively.

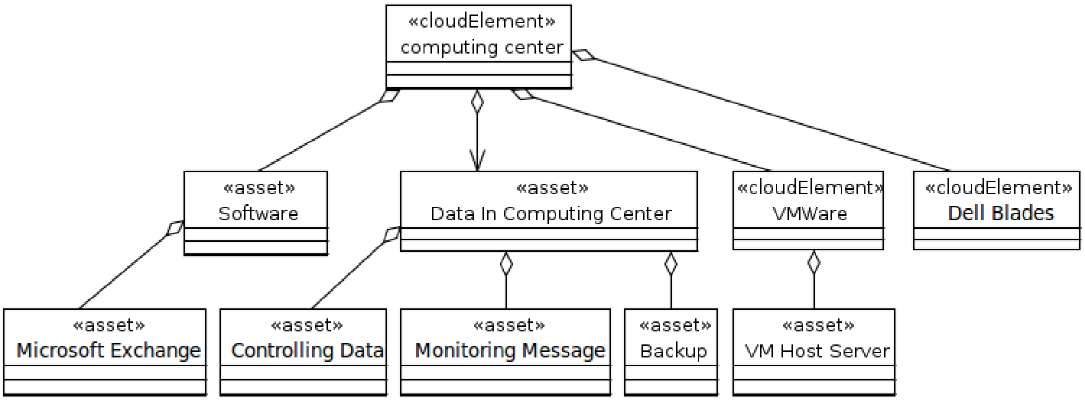


Figure 3: Example of asset refinement

As the CSAP instance is the starting point, we collected all cloud elements being assets and refined them where applicable. We also screened work instructions, organization charts and other business related documents for further assets. Furthermore, we visited the data center of the LANFER SYSTEMHAUS to identify even more assets. Altogether, we identified 105 assets.

In addition, we document

- The owner for each asset. The owner is “responsible” for the asset, e.g. if we consider some data as asset, the owner is responsible to monitor access rights on this data.
- Relations between assets. A relation may describe, e.g. that some software processes some given data.
- The location of assets. For example, the Microsoft Exchange server is located in Datacenter1.
- The asset type. For example, data can be either of type stored data or transmitted data.

For the identified assets we conduct the risk analysis.

3.3. *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 previous threat analyses. We provide a catalog of predefined TP, which were created based on the state of the art works and the experiences of the authors (e.g. (CSA, 2011); (European Network and Information Security Agency, 2009); (Heiser & Nicolett, 2008)). Among others, we have considered the list of seven threats released by the Cloud Security Alliance (CSA) (2011), 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. 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. 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.

The threat patterns are organized according to the categories confidentiality, integrity, and availability.

An example for a TP of the category availability is:

"Unavailability of [*cloud element*] for [*all end customers and cloud customers*]".

To instantiate the threat pattern, the CSAP instance representations of *cloud element* and *all end customers and cloud customers* shall be inserted into the variable text passage. If we instantiate the above given threat pattern for our case study, we get:

"Unavailability of Controlling Data for LANFER SYSTEMHAUS."

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.

Using our catalog reduces the risk that an essential threat is not considered.

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 ISO 27001:2005.

We identify the relevant threats for an asset by selecting the TP that refers to the corresponding asset type. For, e.g. the asset with type stored data, we can select the first TP of our catalog, namely:

"Disclosure of [*stored data*] of [*cloud customer, end customer*] by [*cloud provider, phone support, cloud administrator, cloud developer, third-party provider, other cloud customer, other end customer, external attacker*]“.

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.

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 exploit the vulnerability. Hence, it does not need to be considered in the further risk analysis. Note that we do not have to document a vulnerability if this vulnerability is already addressed by an existing control.

Table 1 depicts the list of existing controls for a subset of the identified assets with regard to confidentiality (C), integrity (I), and availability (A).

Asset	**Existing control (C)**	**Existing control (I)**	**Existing control (A)**
Controlling Data	Access control, server in secured area	Access control, server in secured area	Daily Backups, RAID system
Microsoft Exchange	Server in secured area	Server in secured area	RAID system, CD to install available
Monitoring Message	Only send to limited number of employees	No existing control	Send to more than one employee
Backup	Stores in secured area with restricted access of few employees	Stores in secured area with restricted access of few employees	Representatives
VM Host-Server	No existing control	Server in secured area	Redundant server in secured area

Table 1: An excerpt of identified assets and existing controls

Step 2: Define threat and vulnerability levels: In this step, we determine the likelihood of the threat occurrence for each threat and define the level of vulnerability. The likelihood scale of threats can be classified in *LOW, MEDIUM* and *HIGH* as default values. A *LOW* threat likelihood represents *minor interest of attackers*, whereas a MEDIUM threat likelihood shows a medium interest (e.g. script-kiddies), and a *HIGH* threat likelihood shows a *major interest of attackers to threaten the asset*.

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

In Table 2, we show the results of identifying threats and vulnerabilities for our case study. A "-" means that no threat has been identified so far.

Asset	Threat (C)	Threat (I)	Threat (A)	Vulnerability
Controlling Data	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	gaining access to secured area (C,I,A), ...
Microsoft Exchange	-	Modification of *Microsoft Exchange* by an attacker	Unavailability of *Microsoft Exchange* for LANFER SYSTEMHAUS	impersonating an administrator and installing modified

				Exchange software (I), ...
Monitoring Message	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*	network sniffing to read monitoring messages (C), ...
Backup	Disclosure of *stored backup* of LANFER SYSTEMHAUS by an attacker	Modification of *backup* by an attacker	Unavailability of *backup* for LANFER SYSTEMHAUS	responsible person and all representatives are not available when access to backup is necessary (A), ...
VM Host-Server	-	Modification of *VM host server* by an attacker	Unavailability of *VM host server* for LANFER SYSTEMHAUS	gaining access to secured area (I,A), ...

Table 2: An excerpt of identified assets, related threats, and vulnerabilities

The likelihood of threats and the levels of vulnerability collected in this step will be used in Phase 4 to determine the likelihood for potentially occurring security failures.

3.4. Phase 4: Assess Risks

Risk management is mentioned in sections 4.2.1 e 1 - 4.2.1 e 4 of ISO 27001:2005. In this 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. The management has to commit to this risk acceptance level.

To accomplish this phase, we sub-divide it into the following steps:

Step 1: Assess business impact: This step is concerned with assessing the business impact. It addresses Sections 4.2.1 d 4 and 4.2.1 e 1 of ISO 27001:2005. Business impacts represent consequences that implicate the loss of security goals (e.g., confidentiality, integrity, or availability) of an asset in case of a security incident. A business impact has to be assessed by an impact value.

We propose the following approach to assess the business impact value:

The assessment only considers 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 are 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 level as represented in Table 3. Then, we assess the business impact for each identified asset according to these criteria. In Table 5, we show the estimated business impact level for our case study in the columns marked with 'B.I.'.

Impact level	Description (criteria)
1	no consequence if asset is successfully threatened
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 threatened

Table 3: Business Impact Level Scale

Step 2: Determine security failure likelihood: In this step, which corresponds to Sect. 4.2.1 e 2 of ISO 27001:2005, 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 4. The values are based on the recommendations of ISO27005, Annex E.
In Table 5, we show the estimated likelihood for security failure levels for our case study in the columns marked with 'S.F.'.

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

		attackers have a major interest to threaten asset

Table 4: Security Failure Likelihood Scale (VL: Vulnerability Level, TL: Threat Likelihood)

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 ISO 27001:2005.

Since impact value (Table 3) and security failure likelihood (Table 4) are multiplied to determine the risk level, a risk level equal or below 10 is acceptable according to our level definition.

The reasoning behind this acceptance level is as follows:

- In case of no consequences or consequences that can easily be handled (impact value = 1 or 2), we can accept the risk even if attackers have an interest to threaten the asset and no related controls are in place (security failure likelihood <= 5).
- In case of moderate effort being necessary to handle consequences (impact value = 3), we can accept the risk if the security failure likelihood has the value <=3, but not if no or only basic protection is implemented and attackers have an interest to threaten the asset (security failure likelihood = 4 or 5).
- In case of consequences that can be handled only with high effort or lead to the situation that the survival of the company is uncertain (impact value = 4 or 5), we can accept the risk if attackers have only minor interest or all identified threats are addressed by controls (security failure likelihood = 1 or 2)

Table 5 represents the results of steps 1 (business impact), 2 (security failure), and 3 (risk level) for our example.

Asset	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)
Controlling Data	4	3	2	3	2	2	**12**	6	4
Microsoft Exchange	-	2	3	-	2	2	-	4	6
Monitoring Message	2	2	2	2	5	3	4	10	6
Backup	2	2	3	3	2	1	6	4	3
VM Host-Server	-	1	5	-	3	3	-	3	**15**

Table 5: Business Impact (B.I.), Likelihoods for Security Failures (S.F.), and the Estimated Risk Level (R.L.) for Identified Assets

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 10. If the level of a risk does not correspond to an acceptable risk level, this risk has to be treated. This step corresponds to Sect. 4.2.1 e 4 of ISO 27001:2005. For every risk that needs treatment, the priority for the treatment is deduced by the risk level. 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.

In this article, we focus on treatment 1. Whenever this treatment is selected, we continue with Phase 5. If no further treatment is necessary, we can continue to Phase 7.

3.5. Phase 5: Instantiate Security Requirements

This phase considers all those assets identified in phase 4 having an unacceptable risk level. These assets should be treated. In this phase, we work with the assets that can be treated by selecting controls (see treatment 1) in order to decrease the risk level. To be able to identify new controls, we have to define security requirements. For defining these security requirements, our method uses Security Requirement Patterns (SRP) (Beckers et al., 2013b). These SRP follow the same principles as the already mentioned Threat Patterns. This means the 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 Threat Patterns introduced in phase 3. This means that Threat Patterns are linked to SRP that are relevant for the assets menaced by the described threat.

For the threat

“Disclosure of stored controlling data of LANFER SYSTEMHAUS by an attacker“,

the corresponding requirement

“Preserve confidentiality of stored [data] of [cloud customer, end customer] by preventing disclosure by [cloud provider, phone support, cloud administrator, cloud developer, third-party provider, other cloud customer, other end customer, external attacker]“

can be selected and instantiated as follows (by making use of the threat pattern instantiation):

SR1“Preserve confidentiality of stored *controlling data* of *LANFER SYSTEMHAUS* by preventing disclosure by *an external attacker*.”

Using the mapping between TP and SRP, we select relevant SRP for the assets, which have an unacceptable risk level and instantiate them. In addition to SR1, we defined the following security requirements:

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, etc.) 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*.

The benefit of security requirements is that it is possible to verify whether they have been fulfilled. This fact is used to check if all security requirements for a cloud scenario have been fulfilled. Whenever this is the case, we can state that the chosen security level is sufficient. Whenever a risk remains which has not been addressed, it is necessary to re-evaluate the asset and add security requirements.

3.6. Phase 6: Instantiate Controls

This step considers the treatment of risks by selecting appropriate controls based on the requirements defined in Phase 5. It corresponds to Sect. 4.2.1 f 1 of ISO 27001:2005.

Security requirements have to be fulfilled by controls. The representation of controls in our method is specified by Control Patterns (CP). CPs 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. ISO 27002 provides a reference for selecting controls when implementing an ISMS based on ISO 27001. The structure of CP is specified by a UML meta-model. This makes it possible to extend the CP catalog by new control patterns, whenever necessary.

We have also specified a mapping between our predefined SRP and predefined CP. This means that users have a pre-selection of CP that could be relevant for a certain security requirement. Using this mapping, users can instantiate each CP from this pre-selection 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 the following new controls:

- 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).
- To address the security requirement *SR 2*, cryptographic means for signatures were applied including the necessary measures from ISO 27002:2013 (A.10).
- 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.
- Controls addressing the security requirement *SR 4* (e.g. A.11.1) were already in place (see Table 2).
- To address the security requirement *SR 5*, controls for redundant servers (A.17.2) have to be applied.

After selecting controls it has to be verified if the level of risk has been reduced to an acceptable risk level. This is achieved by performing Phase 4 again.

3.7. Phase 7: Generate Documentation

The final phase of our method is concerned with generating documentation. To obtain the relevant documents for each of our phases, we have to have a look at the output we require in each phase. In detail these are:

Phase 1: CSAP instance
Phase 2: List of identified assets
Phase 3: List of threats and their corresponding vulnerabilities
Phase 4: List of identified risks
Phase 5: List of security requirements
Phase 6: List of controls to be implemented to fulfill the security requirements

All the above-mentioned results are summarized and transferred into a document. This document serves as *Statement of Applicability,* which is required as part of the ISO 27001 ISMS documentation and can be used for a certification process.

4 Lessons learned/Discussion

Applying the CORAS method has turned out to be time-consuming and labor-intensive for an SME such as the LANFER SYSTEMHAUS. As a result, we decided to use the approach presented in this paper, which uses CSAP and a comprehensive hierarchy of assets and related information such as stakeholder, location, asset owner, instead of the asset diagrams of the CORAS method. The process was carried out in this way, i.e., mainly manually, as the tool support was still in its very early prototyping stage. Therefore, only a fraction of the tool support was available at that time.

A risk assessment can be executed either qualitatively or quantitatively (Elky, 2006). We decided to use a quantitative risk assessment, in which risk evaluation criteria and likelihood scales contain numeric values. The reason for that choice is that dealing with numeric values rather than qualitative values is considered more convenient and intuitive for the employees of the involved industrial partner.

Furthermore, we found out - during the risk analysis - that a refinement of assets is very helpful. We believe that such a refinement will help us augmenting the effectiveness of our method and reduce the effort for documenting, even though there were difficulties in finding the right granularity/abstraction level for the asset refinement.

We evaluated our initial asset identification and refinement approach described in Phase 2 and found out that it is possible to refine the assets into five main categories, namely Hardware, Software, Data, Network, and Processes. The evaluation was conducted as follows: a comprehensive list of all assets was compiled. It was then possible to map every asset on this list to the assets refined using the categories. For example, the Exchange Server found on the list is mapped to the asset of the category Software.

Our usage of pattern catalogs has increased our confidence in conducting risk analysis for SMEs, as patterns can easily and intelligibly be selected and instantiated by the employees.

5 Tool Support

The ClouDAT tool is a model-based tool realized using the Eclipse framework (Eclipse, 2014). As Eclipse is realized in Java, which can be used on many different platforms, the ClouDAT tool is also not restricted to a specific OS. Figure 4 gives an overview of the architecture and technologies used.

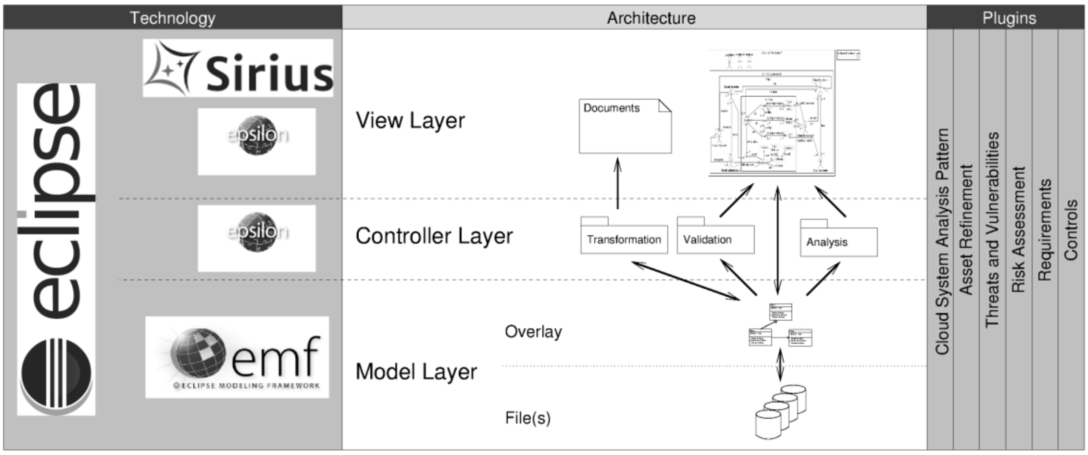


Figure 4 Tool Architecture and Technologies

The ClouDAT tool is modularized along the process steps. This means that for each step a separated eclipse plugin exists. Those plugins can be used in isolation, but they also provide capabilities to integrate all steps. Each plugin itself is further modularized using the model view controller (MVC) (Buschmann et al., 1996) design pattern.

The model definition and storage (model layer) is implemented using the eclipse modeling framework (EMF, 2014). EMF provides capabilities to define meta-models which are then used to generate file structures for storing a meta-model compliant model, an overlay to access such a model programmatically, and tree-editors to create and manipulate a model.

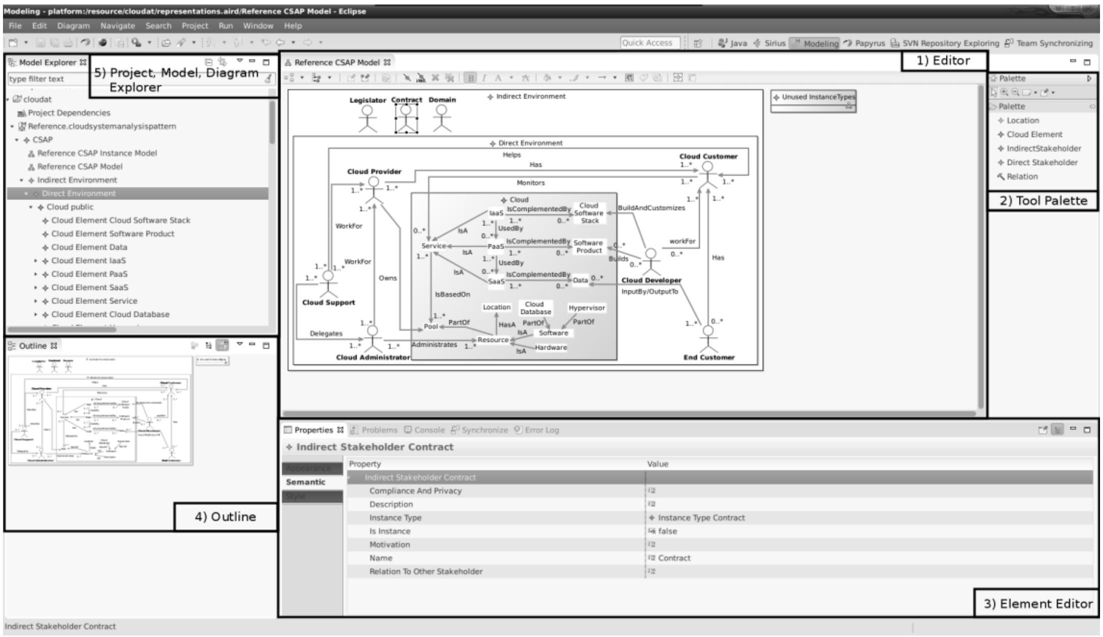
For model generation, validation and analysis (controller layer) several languages of the Epsilon framework (Epsilon, 2014) are used. They offer capabilities

- To transform between different model types using Epsilon Transformation Language (ETL), for example a CSAP model into an according UML representation for further use with other tools,
- For checking a model using Epsilon Validation Language (EVL), for example if a certain information is missing or information in different models are inconsistent,
- For guiding through the population of a model using Epsilon Wizard Language (EWL), and

- For using a model for a certain analysis using Epsilon Object Language (EOL), for example computing risk values.

On top of these layers, the Sirius (Sirius, 2014) framework is used to implement graphical editors (view layer) to create and manipulate the models. Additionally, Epsilon Generation Language (EGL) is used to generate the documentation for the certification as well as documents used to support a certain step.

To enable the integration of the different plugins, all plugins rely on the same basic meta-model, which is extended for each plugin to serve its purpose. As all plugins and the models they produce have a common basis, it is easy to weave them using EMF, Epsilon and Sirius.



Indirect Stakeholder Contract

Property	Value
Indirect Stakeholder Contract	
Compliance And Privacy	
Description	
Instance Type	Instance Type Contract
Is Instance	false
Motivation	
Name	Contract
Relation To Other Stakeholder	

Figure 5 Cloud System Analysis Pattern Editor

Figure 5 shows the Cloud System Analysis Pattern Editor as example for a plugin provided by the ClouDAT tool. This plugin allows to define CSAP models and to instantiate them. The first activity is meant for the rare case that users want to adapt the reference CSAP to the needs of their case, for example by changing the wording. This increases the flexibility of the ClouDAT tool. The second case is the usual one where users facilitate the CSAP to document their cloud scenario.

The tool interface consists of five basic elements. First, the graphical editor itself which supports direct editing of labels, dragging and dropping of elements, adjusting relations and so forth. The graphical representation can be exported to various picture formats. The representation is also part of the certification documentation. Second, the tool palette which is used to create new elements and relations within the editor view. Third, the element editor which is used to add information which is not in the diagram (e.g. properties) to an element. Fourth, the outline which gives a rough overview of the whole diagram. It also allows fast scrolling. Fifth, the project, model, and diagram explorer which allows to browse existing projects, and to browse the models as well as the diagrams contained in the respective projects.

6 Related Work

To the best of our knowledge, there is no other approach combining cloud-specific analysis patterns, threat patterns, security requirement patterns, and control patterns.

CORAS (Lund et al., 2010) 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. (2014b) 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 (Beckers et al., 2014b; Lund et al., 2010) do not consider threats specific to cloud systems, such as those released by the Cloud Security Alliance (CSA) (2011).

Gandhi et al. (2011) provide a method for structuring requirements as well as identifying and representing correlations between requirements. The method considers possible bypassing of requirements due to 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) (Alberts & Dorofee, 2002) 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 (Microsoft Corporation, 2006) 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.

7 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. Currently, the approach is meant to be used by experienced system administrators. They should have no problems to apply our approach.

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
- Tool support for our approach
- Augmenting the effectiveness of applying the method and reducing the documentation effort for SMEs by hierarchical refinement of assets.

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. It is planned to use the tool on the case study of our industry partner LANFER SYSTEMHAUS to evaluate and further enhance it. 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.

Acknowledgements

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 during the identification of assets.

References

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

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, D. A., Rabkin, A., Stoica, I., & Zaharia, M. (2009). *Above the clouds: A berkeley view of cloud computing* (Tech. Rep.). Berkeley: University of California.

Beckers, K., Côté, I., Faßbender, S., Heisel, M., & Hofbauer, S. (2013a). A pattern-based method for establishing a cloud-specific information security management system. *Requirements Engineering, 18*(4), 1-53.

Beckers, K., Côté, I., & Goeke, L. (2014a). A Catalog of Security Requirements Patterns for the Domain of Cloud Computing Systems. In *Proceedings of the 29th Symposium on Applied Computing* (pp. 337-342). New York, NY, USA: ACM.

Beckers, K., Côté, I., Goeke, L., Güler, S., & Heisel, M. (2013b). Structured pattern-based security requirements elicitation for clouds. In *Proceedings of the 7th International Workshop on Secure Software Engineering (SecSE)* (pp. 465-474). Washington, DC, USA: IEEE Computer Society.

Beckers, K., Heisel, M., Solhaug, B., & Stølen, K. (2014b). ISMS-CORAS: A Structured Method for Establishing an ISO 27001 Compliant Information Security Management System. In *Engineering Secure Future Internet Services and Systems, LNCS 8431* (pp. 315-344). Berlin, Heidelberg: Springer Verlag.

Beckers, K., Küster, J.-C., Faßbender, S., & Schmidt, H. (2011). Pattern-based support for context establishment and asset identification of the ISO 27000 in the field of cloud computing. In *Proceedings of the International Conference on Availability, Reliability and Security (ARES)* (pp. 327-333). Washington, DC, USA: IEEE Computer Society.

Buschmann, F., Meunier, R., Rohnert, H., Sommerfeld, P., & Stal, M. (1996). *Pattern-Oriented Software Architecture: A System of Patterns*. John Wiley & Sons.

BSI transition guide. Retrieved October 28, 2014, from http://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf

ClouDAT project. Retrieved October 28, 2014, from http://www.cloudat.de

Cloud Controls Matrix (CCM). Retrieved October 28, 2014, from https://cloudsecurityalliance.org/research/ccm

Cloud IDC. Retrieved January 14, 2014, from https://www-304.ibm.com/isv/library/pdfs/cloud_idc.pdf

CSA. (2011). *Security guidance for critical areas of focus in cloud computing* (v. 3.0).

Eclipse Framework. Retrieved October 28, 2014, from http://www.eclipse.org

Eclipse Modeling Framework (EMF). Retrieved October 28, 2014, from http://www.eclipse.org/modeling/emf

Epsilon Framework. Retrieved October 28, 2014, from http://www.eclipse.org/epsilon

Elky, S. (2006). An Introduction to Information Security Risk Management. Retrieved October 28, 2014, from http://www.sans.org/reading-room/whitepapers/auditing/introduction-information-system-risk-management-1204

European Network and Information Security Agency. (2009). *Cloud computing – benefits, risks and recommendations for information security*.

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

Gandhi, R. A., & Lee, S. W. (2011). Discovering multidimensional correlations among regulatory requirements to understand risk. *ACM Transactions on Software Engineering Methodology, 20*(4), 1-37.

Heiser, J., & Nicolett, M. (2008). *Assessing the security risks of cloud computing.*

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). (2005). *ISO/IEC 27001: Information technology – Security techniques – Information security management systems – Requirements*.

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). (2011). *ISO/IEC 27005: Information technology – Security techniques – Information security risk management.*

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). (2013). *ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security controls.*

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). (2013). *ISO/IEC: 27001: Information technology – Security techniques – Information security management systems – Requirements*.

LANFER SYSTEMHAUS. Retrieved October 28, 2014, from http://www.lanfer-systemhaus.de

Lund, M. S., Solhaug, B., & Stølen, K. (2010). *Model-Driven Risk Analysis. The CORAS Approach.* Berlin, Heidelberg: Springer Verlag.

Mell, P., & Grance, T. (2011). *SP 800-145. The NIST definition of cloud computing.* Gaithersburg, MD, United States: National Institute of Standards and Technology (NIST).

Microsoft Corporation. (2006). *The security risk management guide*. San Francisco, California, USA.

Sirius Framework. Retrieved October 28, 2014, from http://www.eclipse.org/sirius

Bios

Azadeh Alebrahim is a research assistant at paluno - the Ruhr Institute for Software Technology, University of Duisburg-Essen, Germany. Her main research interests include quality-based and pattern-based software development, requirements engineering, and software architecture with regard to security.

Isabelle Côté is currently working at ITESYS - Institut für technische Systeme GmbH as a safety/security consultant and project manager. In 2012, she received her Doctorate (PhD) in computer engineering from the University of Duisburg-Essen. Her research interests include requirements engineering and design and verification of dependable systems.

Stephan Faßbender is a research assistant at paluno - the Ruhr Institute for Software Technology, University of Duisburg-Essen, Germany. His research interests include compliance, privacy, security, and service-oriented architectures (SOA).

Ludger Goeke graduated from the Dortmund University of Applied Science and Arts in 2007. He currently works as a consultant at ITESYS - Institut für technische Systeme GmbH.
His research interests include security, requirements engineering, design implementation and verification.

Denis Hatebur is CEO of ITESYS - Institut für technische Systeme GmbH since 2003. He conducts projects in the field of security and safety. Since 2005, he also works at the University of Duisburg-Essen. In 2012 he received his PhD in computer/software engineering. His research interests include requirements engineering, design and verification of dependable systems.

Response to reviewers

Explain, in a point-by-point manner, how you have addressed the reviewers' comments in preparing the final camera-ready copy of your conference/workshop paper

Our responses to this point are included with the answers to the next point.

Explain how you have extended the paper with 30% new or modified content.

To illustrate our extensions, we divided our contribution into the following categories:

Modified content:

- We changed the title.

This addresses review comment no. one of reviewer no. four.

- We provided more details on the ClouDAT framework and its current status in section The ClouDAT framework.

This addresses review comment seven of reviewer no. four as well as review comment two of reviewer no. two.

- We added an example of a CSAP instance to the paper with additional information to point out that the methodology indeed focuses on cloud systems in the section on the cloud system analysis pattern.

This addresses reviewer comment two of reviewer no. one.

- We added an example for an SRP instance to section 2.3.

- We added information from where we got the information for our case study in section 3.1.

- We restructured section 3.7 to make it easier to read.

Modified and new content:

- We revised the introduction about our previous work in Beckers et al. and its relation to the work in this journal. We also stated the relation of our methodology to the ISO27005 standard. It now provides more details on how our risk assessment method is related to the work presented in Beckers et al. and why and how it differs. We also added a paragraph describing why the example/case study is rather generic. However, we tried to provide more specific examples within our given / allowed margins to increase the relations between example and case study.

With these modifications / additions we address review comments one and two of reviewer no. in more detail / with additional details.

- We re-wrote most of section 3.2 and added information on how the initial asset identification was performed and how the refinement was performed. The refinement process as such was revised based on the experiences we gained from the initial process.

This addresses review comment eight of reviewer no. four.

- We added some examples and explanatory texts to section 3.3 and revised some paragraphs to make the complete section more comprehensible.

- For step 2 of section 3.3: We took the advice on the likelihood into consideration and evaluated the possibility of more levels. It became apparent that a third level in the scale is desirable. The new scale now works on three levels, LOW, MEDIUM and HIGH. As a consequence of this adaptation, we modified the corresponding step to treat the new scale.

This addresses review comment nine of reviewer no. four.

- In section 3.4 we adapted the procedure incorporating the new likelihood scale. We also restructured the section describing asset identification and refinement and added a rationale why / when the risk-acceptance levels are considered as "acceptable".

This addresses review comment four of reviewer no. two.

- We revised section 3.5 and added details (including examples) on how TP and SRP are linked.

This addresses review comment three of reviewer no. two.

- We revised the conclusion to reflect the changes made in the work.

New content:

- We added a chapter on lessons learned/discussion to provide more insight on the application of our method. It illustrates the experiences and observations made during the initial application of our method to the LANFER SYSTEMHAUS case study. The lessons learned enabled us to refine the current version of the methodology and to improve its usability.
- We added a chapter on tool support.