Supporting the Security Certification and Privacy Level Agreements in the Context of Clouds

Amir Shayan Ahmadian[1], Fabian Coerschulte[1], and Jan Jürjens[1,2(✉)]

[1] Institute for Software Technology, University of Koblenz-Landau, Koblenz, Germany
ahmadian@uni-koblenz.de, fabian.coerschulte@tu-dortmund.de
[2] Fraunhofer Institute for Software and Systems Engineering ISST, Dortmund, Germany
jan@jurjens.de
http://jan.jurjens.de

Abstract. Outsourcing services into the cloud is a worthwhile alternative to classic service models from both a customers and providers point of view. Therefore many new cloud providers surface, offering their cloud solutions. The trust and acceptance for cloud solutions are however still not given for many customers since a lot of security incidents related to cloud computing were reported. One possibility for companies to raise the trust in the own products is to gain a certification for them based on ISO27001. The certification is however a large hurdle, especially for small and medium enterprises since they lack resources and know-how. In this paper we present an overview of the ClouDAT framework. It represents a tool based approach to help in the certification process for cloud services specifically tailored to SMEs.

Keywords: Cloud computing · Certifying cloud providers · Risk analysis methods · Risk treatment methods · Privacy level agreements

1 Introduction

Cloud computing is a business model that kept gaining importance in the recent years. The National Institute of Standards and Technology describes cloud computing as "ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [25]. Cloud computing provides a very interesting opportunity for IT enterprises to service a large amount of customers by offering dynamic scalability, elasticity, and a cost model that is based on pay-as-you-go model.

This research was partially supported by the research project Visual Privacy Management in User Centric Open Environments (supported by the EU's Horizon 2020 programme, Proposal number: 653642).

B. Shishkov (Ed.): BMSD 2015, LNBIP 257, pp. 80–95, 2016.
DOI: 10.1007/978-3-319-40512-4_5

The utilization of cloud computing services has been ever growing in the past years and the growth of this business model is expected to continue in the near future [2]. However, the acceptance of cloud computing is growing slowly, due to the fact that cloud computing introduces new threats and vulnerabilities. Therefore, besides all the advantages of cloud computing, cloud providers need to convince the cloud customers of security.

A possible way to encounter scepticism and raise acceptance is the certification of cloud providers according to standards like ISO27001 [16]. However, for small and medium-sized enterprises (SMEs), offering cloud solutions is a rather complex task, due to the lack of know-how and resources to conduct an ISO27001 compliant risk assessment and generate the appropriate documentation to reach the certification. The ClouDAT project [9] offers a framework helping SMEs handling the certification process. It contains a cloud-specific risk assessment process and allows the automatic generation of ISO27001 compliant documentation based on the outcomings of the risk assessments.

In Sect. 2 we present a high-level overview of ClouDAT and introduce the risk analysis process. In Sect. 3 we deliver an in-depth insight into the underlying metamodel to introduce the key concepts of ClouDATs risk analysis. Based on this insight, Sect. 4 gives a detailed introduction into the methodology associated with the metamodel to point out the benefits that ClouDAT offers SMEs. Moreover, in Sect. 5, we introduce UMLsec [21], an extension of UML for secure system development, along with the CARiSMA [4] tool that supports UMLsec models. Section 6 provides an introduction to the use of formalized privacy level agreements in conjunction with ClouDAT framework. in Sect. 7 a conclusion is provided.

2 The Security Certification Approach

In the first step we introduce the structure of the ClouDAT framework and outline its risk analysis process.

2.1 The ClouDAT Framework

The result of the ClouDAT project [9] is the ClouDAT framework. This framework is available as open source and supports SMEs by providing a means for certifying cloud services. Generally, the ClouDAT framework establishes an Information Security Management System (ISMS) based on the ISO 27001 [16] standard. The development of an ISMS allows organizations to implement a framework for managing the security of their information assets such as financial information, employee and customer information. The framework contains different parts:

- A metamodel for the risk analysis process complying with ISO 27001 standard.
- A metamodel for the risk treatment process complying with ISO 27001 standard.

– A catalog of security requirements.
– A catalog of cloud-specific threats.
– A catalog of security controls.
– Different editors to model cloud environment and use cases, security requirements, and security controls.

In the rest of this section, the above mentioned parts are described along with the ClouDAT risk analysis process. The metamodels are introduced in the respective sections.

2.2 The Overview of the ClouDAT Risk Analysis Process

Figure 1 [1] presents an overview of the our risk analysis process, which complies with ISO 27001 standard. In the following, we summarize the different phases of the process.

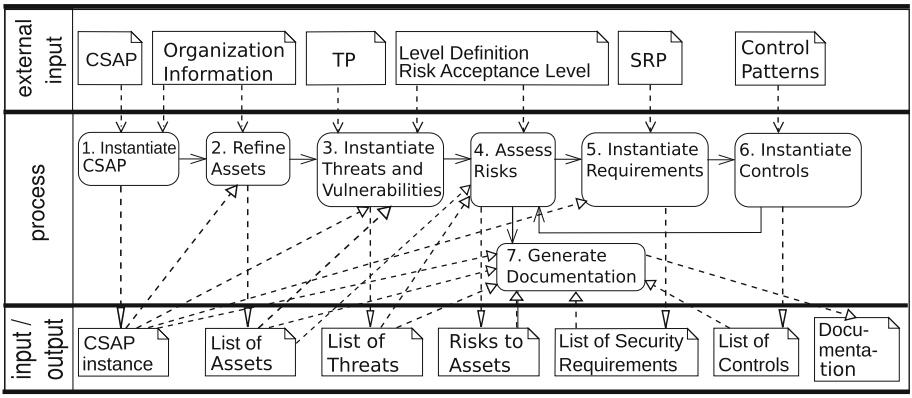

Fig. 1. Risk analysis process

Cloud Elements Identification. In this phase, the scope and the boundaries of the ISMS is defined. To this end, we employ the Cloud System Analysis Pattern (CSAP) [3]. CSAP provides a structured approach to describe cloud environments. It provides a framework to model their elements, such as data elements, physical objects, and stakeholders. Moreover, it describes the relations between the cloud elements.

The process of the asset identification starts with instantiating the CSAP. In the first step, the cloud customers and the required cloud services are identified. Then the cloud is instantiated, which consists of different types of cloud elements.

Refine Cloud Elements. This phase complies with Sect. 4.2.1 d of the ISO 27001 standard. The main goal of this phase is to determine the cloud elements that are important to the risk analysis. Later, for these cloud elements, the risk analysis is performed. The results of this phase are collected in a table, which is called *cloud element list*. This table contains all mandatory cloud elements for the risk analysis.

The cloud elements refinement is performed in two steps [1]:

- Refine cloud elements and their location: In this step the abstract mandatory cloud elements are refined into more concrete and detailed cloud elements. Moreover, the location of the cloud elements are identified.
- Assign responsibilities and relationships: In this step the responsibilities of the cloud elements are identified and the relations between the cloud elements are determined.

Instantiate Threats and Vulnerabilities. In this phase, for all the cloud elements that were specified in the previous phase a threat analysis is performed. Generally, in the threat analysis, it is investigated whether a cloud element is endangered. Moreover, it is examined if a cloud element has vulnerabilities that can be exploited by a threat. In the ClouDAT framework a catalog of predefined threats and vulnerabilities for cloud elements is provided. This catalog is based on previous works, for instance [5,11,14]. Additionally, the list of cloud computing top threats [6] from Cloud Security Alliance (CSA) is considered. The provided catalog is a starting point for the threat analysis and should not be considered as complete.

Assess Risks. This phase complies to sect. 4.2.1 of the ISO 27001 standard. The results of this phase declare the existing risk to the cloud elements, and specify whether a cloud element requires risk treatment. Before starting the risk analysis, the risk approach and the risk acceptance level must be specified. Generally, the risk assessment is based on the business impact, and the security failures. Business impacts express the consequences that affect the failure of the security goals. Furthermore, considering the threats and the vulnerabilities that are identified in the last phase, we need to determine the likelihood of potential security failures for all menaced cloud elements.

The multiplication of the likelihoods for the security failures and the values that are assigned to the business impacts estimates the risk levels of the cloud elements. By comparing the estimated risk levels of cloud elements and the defined risk acceptance level, the cloud elements that require risk treatment are identified.

Instantiate Security Requirements. In this phase we consider all the cloud elements with an unaccepted risk level. We need to define a risk treatment method to reduce the risks. We comply with ISO 27001 Sect. 6.1.3 by defining and applying an information security risk treatment process. The ISO 27001 specifies the following treatments:

– Applying appropriate controls.
– Accepting risks.
– Avoiding risks.
– Transferring the associated business risks to other parties.

In Sect. 4 we describe our risk treatment method completely. In this section, we only summarize our method. Generally, if a cloud element has an unacceptable risk level, security requirements have to be defined. To this end, security requirement patterns (SRP) are defined (Sect. 3). In a concrete certification process, security requirement patterns are instantiated, and for each cloud element with an unaccepted risk level, a security requirement will be defined. ClouDAT framework provides a catalog of predefined SRPs.

Instantiate Controls. Our risk treatment process complies with ISO 27001, and mainly contains applying appropriate security controls considering the security controls provided in Annex A of the ISO 27001. Generally, the selection of the controls is based on the cloud elements with unaccepted risk level, which are identified during risk assessment. Similar to security requirement patterns, the representation of the security controls is specified by control patterns (CP), and a catalog of predefined security controls is provided. As we mentioned above, we describe our risk treatment method in more details in Sect. 4.3.

Generate Documentation. In the final phase of our risk analysis process, a document is generated. This document contains the list of refined cloud elements, the list of threats and corresponding vulnerabilities, the list of cloud elements with unaccepted risk level, the list of security requirements, and finally the list of selected controls to reduce the identified risks. The resulting documentation is used as a reference for the certification. In the following sections, we describe the underlying concepts of the risk analysis process in more details together with the basic metamodels.

3 Risk Analysis Metamodel

This section describes the foundations of the risk analysis process in detail. Therefore, it takes a closer look at a simplified version of the risk analysis metamodel defined by the ClouDAT process.

Figure 2 shows an excerpt of the full risk analysis metamodel class diagram. Since we only want to discuss the key concepts, this illustration hides several classes and additional implementation detail.

The goal of the risk analysis phase is to identify the risks affecting the cloud elements that were found during the "Cloud Elements Identification" phase (see Sect. 2.2 and [1]). The central element for this step of the ClouDAT approach is the CloudElement. This can basically be anything of value to the company; from documentation to real physical systems. A cloud element is identified by a

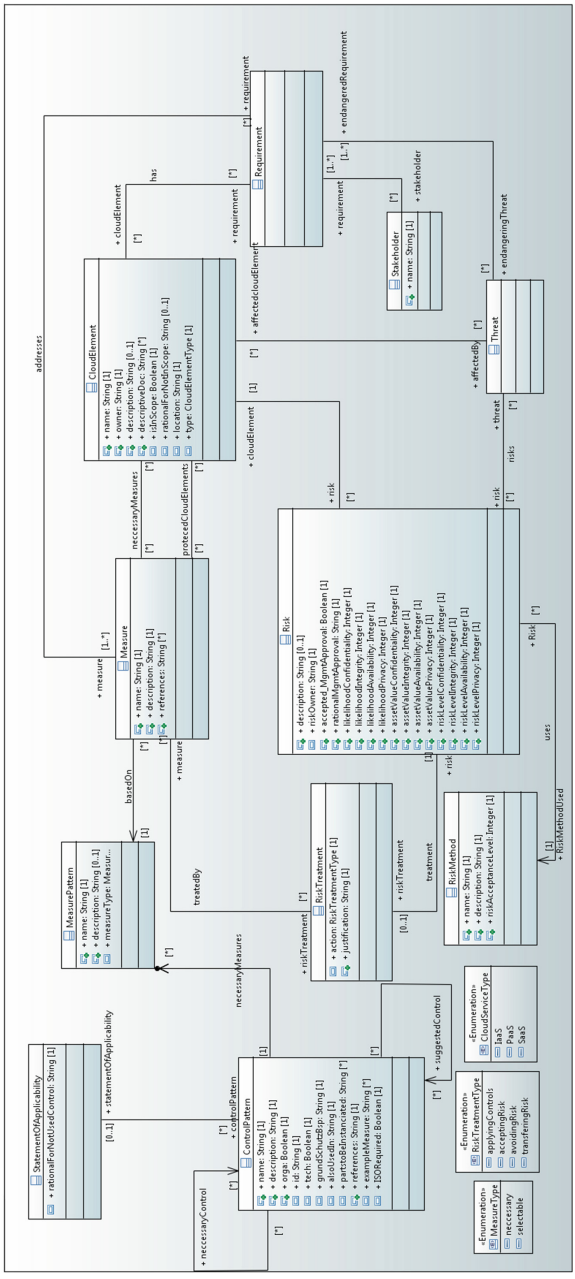

Fig. 2. Risk analysis metamodel excerpt

unique name und contains additional information such as type, owner, descriptions and a location. Additionally it can be excluded from the scope of the risk analysis once a convincing explanatory statement (rational) for this case is given.

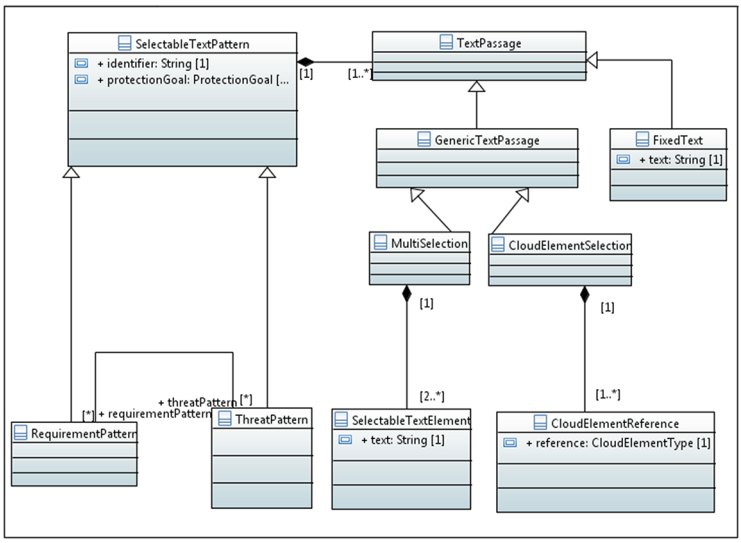

Fig. 3. Selectable text metamodel.

CloudElements can be subject to requirements verbalized by stakeholders. The requirements are expressed using ClouDATs pre-defined RequirementPatterns illustrated in Fig. 3. They consist of fixed text passages and generic text passages. Fixed text passages represent the meaning of a security requirement and can not be edited by the user. Generic text passages can for example be multi selections or relations to specific cloud elements. The requirement patterns can be seen as clozes the user has to fill out in order to instantiate a certain requirement.

Figure 4 illustrates an example requirement. It consists of fixed text and multi selections. The elements in squared brackets represent the different options for a multi selection. Since Fig. 3 provides a sufficient understanding of the concepts, Fig. 2 does not show additional implementation detail for the instantiation of requirements based on requirement patterns, thus showing only the requirement class.

Requirements can be endangered by threats that are based on ThreatPatterns defined by the ClouDAT framework. The ThreatPatterns are shown in Fig. 3 and are very similar to RequirementPatterns. Figure 5 shows an example for a threat pattern defined by ClouDAT. Since the threats indirectly endanger the CloudElements, there is also an association to it.

The presence of threats entails risks. While threats are very abstract and by themselves propose no danger to a company, risks do. A risk represents the

The cloud computing system shall ensure that a
[cloud customer, end customer, administrator]
only has the permissions of the assigned roles for
[cloud service]

Fig. 4. An example of security requirement pattern.

Disclosure of communication between the
[cloud service] and the
[cloud customer, end customer, administrator]
for example by network sniffing or gaining access to relevant areas.

Fig. 5. An example of threat pattern.

"potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization" [15]. The risk class contains a description, which serves as unique identifier for a risk and a risk owner, which is the person responsible for a given risk. It is also possible, that a risk is accepted by the management without further treatment (acceptedMgmtApproval). This case however demands for a convincing explanatory statement (rationalMgmtApproval). Furthermore a risk consists of likelihoods, business impacts (assetValue) and the resulting risk levels for the protection goals confidentiality, integrity, availability and privacy. Since a certification requires every risk to be handled or accepted, it is mandatory to deliver an acceptance rule for every risk. The acceptance rule is called RiskMethod in ClouDAT, and contains a name, description and riskAcceptanceLevel. The acceptance level can be seen as a threshold not to be exceeded by risks using the RiskMethod.

The risks exceeding the acceptance level have to be treated by the user. Therefore ClouDAT allows the definition of RiskTreatments that consist of a treatment action and a justification that explains, why a certain action has been taken. ClouDAT allows to treat a risk by applying controls, accepting the risk, avoiding the risk or transfering the risk. In case a risk is treated by applying controls, the user has to specify the measures that were used to reduce the risk.

ClouDAT distinguishes between controls and measures. A control describes an action that can be taken to reduce a risk but is defined on a very abstract level, while a measure is a concrete implementation of a control. A control for example is "Asymmetric encryption" and a possible measure based on this control could be the implementation of a specific encryption protocol like RSA.

The class ControlPattern allows the definition of controls and consists of an id, name, description and indicators whether it is required by ISO27001 or it is an organizational or a technical control. Furthermore it is possible to provide example measures or an example for the control based on the IT-Grundschutz. Controls can also suggest the use of other controls or require the implementation of other controls. For example, the control "Password management system"

requires the implementation of a "User registration and de-registration" system and suggests the "Use of secret authentication information". CloudDAT provides an extensive list of possible controls based on the ISO27001 (see Sect. 4).

A control can provide MeasurePatterns which can be seen as implementation possibilities for the given control. A MeasurePattern consists of a name, description and an indication whether the Measure is neccessary to implement the control or just a selectable implementation method. The concrete instantiation of a MeasurePattern is a Measure, that is associated with requirements and CloudElements.

4 Risk Treatment Method

As we mentioned in Sect. 2.2, our risk treatment method complies with the ISO 27001 and is specified with four different treatment methods, applying appropriate controls, accepting risks, avoiding risks, and transferring the associated business risks to other parties.

According to the ISO 27001 Sect. 6.1.3, considering the risk assessment results, an appropriate security risk treatment option must be selected. To this end, all the security controls that are necessary to the risk treatment must be determined. Afterwards, a comparison of the determined controls with those in the ISO 27001 must be performed, verifying that no mandatory controls have been excluded. Subsequently, a statement of applicability that incorporates the mandatory controls and explanations for inclusions and exclusions of the controls must be provided. In the following sections, we describe these steps in more details.

4.1 Security Controls

In order to apply appropriate controls, we need to specify a list of security controls, from which the proper security controls are selected to reduce the risks of the organization."Controls include any process, policy, device, practice, or other action which modify risks" [17]. The Annex A of the ISO 27001 standard provides the normative controls of the standard. Different international organizations have provided governance documents such as the NIST-SP800-53 [26], the DISA Secure Application Security Technical Implementation Guide (STIG) [10], and the Cloud Security Alliance Cloud Control Matrix (CCM) [8]. In such documents, a set of security controls are collected. Likewise, in the course of ClouDAT project, we provide a control list. The control list contains:

- Security controls of ISO 27001 standard.
- Self-defined security controls: Security requirements have to be fulfilled by controls, hence to cover all security requirements we have defined a few security controls additionally.
- Security patterns: A security pattern, using some security mechanism, describes a solution to the problem of controlling a set of threats. We consider some of the security patterns, which are provided in [12], as security controls.

4.2 The Structure of the Control List

Figure 6 presents a snapshot of the control list. Due to the lack of space, we do not show the whole table. The control list is simply a table which contains all above mentioned security controls. For each control a set of aspects are defined. In the following, we describe these aspects.

ID (ISO 27002)	Control/Measure —Text (ISO 27002)	Dependencies	Req (Ausarbeitung)	Protected Cloud Element
A.5.1.2	Review of the information security policy.	5.1.1 necessary	- referenced indirectly from Security Management and others	generic
A.6.1.1	Information security roles and responsibilities	A.9.2.3 necessary A.5.1.1 necessary	- referenced indirectly from Security Management and others	generic
A.6.1.2	Segregation of duties	5.1.1 necessary	Security Management 7 Security Management 15	generic
A.6.1.3	Contact with authorities	Necessary: A.6.1.3	Security Management 18	generic
A.6.1.4	Contact with special interest groups	-	- referenced indirectly from Security Management	generic
A.6.1.5	Information security in project management	Necessary: 25.4		generic

Fig. 6. A snapshot from the control list.

- ID: The documented controls presented in control list are generally based on the security controls provided in annex A of ISO 27001, and Sects. 5 to 18 of ISO 27002 respectively. These controls are identified by the same ID as in the ISO documents. In the cases, which the standards do not provide appropriate controls, self-defined controls are provided, with the IDs beginning at 19.1 in order to avoid conflicts with the ISO controls.
- Control Text: A short title for the control. For ISO controls, the title matches the one in the original document. Self-defined controls are labeled similarly.
- Dependencies: This entry gives a list of other controls. Mainly two kinds of dependencies are defined:
  - Necessary: The other control should be implemented as well in the most cases. If the user chooses not to apply the necessary control, the reason must be justified.

  - Suggested: The other control might be useful to support the current control or its measure. The tool offers these controls as an option to the user.
- ISO 27001 - 2005 reference: The controls are based on the ISO revision of 2013. For the controls that have equivalent controls in the version 2005, the ID is given respectively.
- Security Requirement: List of relevant security requirements.
- Refinement of (ID): A reference to the control, which is refined by the provided control.
- Refined by (ID): A reference to the control, which refines the provided control.
- Protected Asset: List of the assets, which are protected by the provided control.
- Instance Type: The instance type of the control, when it is possible.
- Asset necessary to perform control with relevant security aspect: The implementation of a control can lead to the creation of additional assets, that need to be protected accordingly.
- BSI References: The related entries from the BSI Grundschutz catalogues.
- Also used in: List of similar controls from CCM (Cloud Control Matrix).
- Technology/Organization: Each control is classified whether it is primarily (+) or supportively (∼) technical or organizational.
- Description of control: A textual description of the control.

4.3 Risk Treatment Process

In Sect. 2.2, we described that after risk assessment, for the cloud elements with unaccepted risk level, appropriate security requirements are elicited. In the control list for each control a set of security requirements are specified. This mapping between controls and requirements simply indicates, which control fulfills which security requirement. Consequently, according to the elicited requirements, we can determine the necessary controls to reduce the risks. In this process the dependencies between the controls are considered.

After the selection of the controls, we need to verify whether the risk levels of the cloud elements are reduced. To this end, we need to perform the risk assessment for particular cloud elements to check whether the controls reduce the risk levels or a modification of the controls or other controls are required. This process is iterated until there exists no cloud elements with an unaccepted risk level. However, sometimes we need to avoid or ignore the risk. Or alternatively, we need to transfer the risk to other parties. These decisions are manually made by the security analyzer and must be reasoned.

Furthermore, we need to provide a statement of applicability (compliant with Sect. 6.1.3 c-d of the ISO 27001). To this end, we have provided a template. This template is simply a table, in which for each selected control either must be justified why the control is excluded, or the overview of the implementation is provided, i.e. the necessary and suggested controls to perform the control are listed.

As an example for the risk treatment process, consider the case, in which the confidentiality of the personal data in a organization, for which we have

have performed the risk analysis, is threaten. In Sect. 3, we have introduced the security requirement patterns. In our SRP catalog such a pattern exists:

"Confidentiality of personal data of [cloud customer, end customer] shall be achieved."

As we have already mentioned, a SRP has variable and fixed text passages. To instantiate the security requirement pattern, from the list of identified and refined cloud elements, an element as a representation of the cloud customer or end customer must be inserted into the variable text passage. Assume that the name of the Organization is *Organization A*, then the instantiated requirement is:

"Confidentiality of personal data of Organization A shall be achieved."

Using the provided mappings between security requirements and security controls in the control list, we select the relevant control:

"To address the security requirement, we apply the controls of the ISO 27001, e.g. access control policy (A.9.1.1), working in secure areas (A.11.1.5), network controls (A.13.1.1), including the controls that are specified as necessary to perform along with mentioned controls."

5 CARISMA, An External Security Analysis Tool

Along the risk assessment process, which is provided by the ClouDAT framework to certify cloud providers and generate documentation, the ClouDAT framework offers the functionality to analyze different cloud services and softwares with the help of external security analysis tools. For instance, consider the case, in which the cloud provider uses self developed cryptographic protocols instead of the standard protocols. In this case, an external tool for analyzing the protocols is needed. An appropriate external tool with different functionalities for security analysis is the CARiSMA tool framework. It offers different automatic verification plugins of UML diagrams for critical requirements. Generally, it provides automated analysis of UMLsec [21] models for security requirements.

UMLsec is an extension of UML in form of an UML profile that provides model-driven development for secure information systems [13]. It can be used to express security requirements within UML diagrams (such as secure information flow [19]). Tags and stereotypes are used to express security requirements and assumptions on system environments. Moreover, constraints are used to determine whether requirements are satisfied by the system design UMLsec [21].

The UMLsec approach has been used in a number of applications [20,23,24].

System security analysis using UMLsec requires an architectural analysis of the software system. To this end, all the components, objects, cloud elements, and the dependencies between them are needed.

In the case of a legacy system, these can be extracted from the code base using techniques for program comprehension such as [27].

In a certification process, it is possible to use different CARiSMA plugins as external tools for security analysis. For instance, we consider Control A.9.1.1 from ISO 27001 standard. It states, that an access control policy based on business and information security requirements must be established, documented,

and reviewed [17]. There exists different approaches to establish access controls. Generally, an access control method restricts the access to information and information processing facilities. If a cloud provider requires an external tool to control the access to information, the RABAC analyzer plugin of the CARiSMA can be used [4]. This plugin is based on the concept of Role Attribute Based Access Control (RABAC) [18], and is implemented and integrated to the ClouDAT framework for the access control analysis in cloud environments.

Above, we mentioned that a cloud provider may need an external tool to analyze cryptographic protocols. CARiSMA offers Sequence Diagram Crypto FOL-Analyzer [22] for security analysis of cryptographic protocols. This plugin as an input receives a protocol, which is expressed as an UML sequence diagram, and performs the analysis.

The CARiSMA website [4] provides more information about the different plugins for the security analysis.

6 Privacy Level Agreement

In this section, we describe how Privacy Level Agreements (PLAs) in conjunction with ClouDAT framework can be used to assist the small and medium cloud providers to ensure security and privacy levels in their services. In the course of VisiOn[1] project and our current research, we develop a visual privacy management platform, which allows the citizens, who communicate with public administration authorities, to achieve desired levels of privacy by creating and monitoring a personal privacy level agreement. A PLA as an appendix to a service level agreement (SLA) describes the level of privacy protection that a service provider will maintain. Cloud Security Alliance (CSA) provides a PLA outline for cloud service providers, in which information privacy and personal data protection practices are addressed. PLA outline intends to provide a possibility to determine a guideline of essential personal data protection legal requirements, to achieve a baseline of compliance with mandatory personal data protection legislation across the EU. Moreover, in a structured way, verify the level of personal data protection offered by different CSPs [7].

In each document generated by the ClouDAT framework to assist the SMEs in the process of certifying their services, valuable information on threats, vulnerabilities, risks and security measures are provided. According to the PLA outline, such information are also needed to create PLAs. Thus, the document generated by ClouDAT can be used as an input to create PLAs. To this end, a formal description of PLA outline is required. Therefore, in our current research we intend to provide a metamodel based on the metamodel provided in Fig. 2. In this way, in a structured way first we specify the PLA outline (in XML format), and afterwards we can automatically generate some parts of the PLA regarding the relevant information provided by ClouDAT framework.

[1] http://www.visioneuproject.eu/.

The overall approach, how a PLA can be generated formally is provided in Fig. 7. According to this figure, in addition to the ClouDAT framework, a questionnaire is used to generate the other parts of the PLA such as the cloud provider information, the data protection inquiries, the data processing methods, and personal data location. This questionnaire is a simple application, for which a set of predefined questions are provided. Different other external tools such as security analysis or threat analysis tools may be also used to generate different sections of the PLA. After generating the PLA, a textual format of the PLA will be provided.

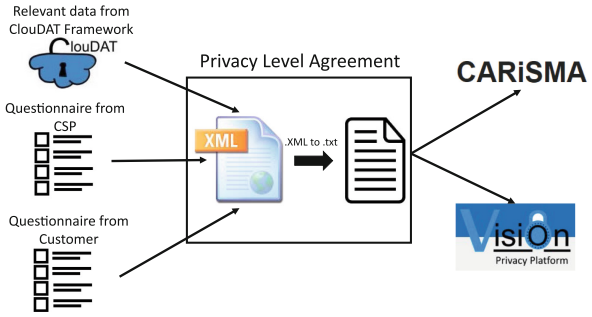

Fig. 7. Overall approach to generate a formalized PLA

The generated PLA can be used for different purposes. In our research, we plan to use the PLA as an input to CARiSMA to perform different security and privacy checks. To this end, currently we are developing new concepts and security checks, for which the infomration provided in the PLA are used as inputs.

7 Conclusions

The certification of cloud computing infrastructures is a very complex task for small and medium-sized enterprises. It requires a lot of effort to be taken because it is mandatory to do a detailed risk assessment and analysis and create detailed documentation of the efforts taken. ClouDAT provides a full fledged framework to support small and medium-sized enterprises in the cloud system certification process based on ISO27001. It consists of a detailed workflow on how to conduct the risk analysis and contains detailed lists of assets, requirements, threats, risks and controls to support the user during assesment phases. ClouDAT allows the user to analyse a modeled scenario both using integrated analysis methods and external analysis tools, thus exposing potential certification problems during analysis. Furthermore ClouDAT allows the automatic generation of ISO27001 compliant certification document, which helps the user in the certification process.

References

1. Alebrahim, A., Hatebur, D., Goeke, L.: Pattern-based and ISO 27001 compliant risk analysis for cloud systems. In: 2014 IEEE 1st Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE), pp. 42–47, August 2014
2. 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.: Above the clouds: a berkeley view of cloud computing. Technical report UCB/EECS-2009-28, EECS Department, University of California, Berkeley. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html
3. Beckers, K., Schmidt, H., Kuster, J., Fassbender, S.: Pattern-based support for context establishment and asset identification of the ISO 27000 in the field of cloud computing. In: 2011 Sixth International Conference on Availability, Reliability and Security (ARES), pp. 327–333, August 2011
4. CARiSMA: Carisma framework, May 2015. https://www-secse.cs.tu-dortmund.de/carisma/
5. Cloud Security Alliance: Security guidance for critical areas of focus in cloud computing v3.0 (2011). https://downloads.cloudsecurityalliance.org/initiatives/guidance/csaguide.v3.0.pdf
6. Cloud Security Alliance: The notorious nine cloud computing top threats in 2013, February 2013. https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/
7. Cloud Security Alliance: Privacy level agreement: A compliance tool for providing cloud services in the European union, February 2013. https://cloudsecurityalliance.org/download/thenotorious-nine-cloud-computing-top-threats-in-2013/
8. Cloud Security Alliance: Cloud Control Matrix (2014). https://downloads.cloudsecurityalliance.org/initiatives/ccm/ccm-v3.0.1.zip
9. ClouDAT: Cloudat project, May 2015. http://ti.uni-due.de/ti/clouddat/de/
10. DISA: Application Security and Development STIG V3 R10 (2015). http://iase.disa.mil/stigs/Documents/U_Application_Security_and_Development_V3R4_STIG.zip
11. European Network and Information Security Agency: Cloud computing - benefits, risks and recommendations for information security (2009). https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security
12. Fernandez-Buglioni, E.: Security Patterns in Practice: Designing Secure Architectures Using Software Patterns, 1st edn. Wiley, New York (2013)
13. Fernández-Medina, E., Jürjens, J., Trujillo, J., Jajodia, S.: Model-driven development for secure information systems. Inf. Softw. Technol. **51**(5), 809–814 (2009)
14. Heiser, J., Nicolett, M.: Assessing the security risks of cloud computing, June 2008. https://www.gartner.com/doc/685308/assessing-security-risks-cloud-computing
15. ISO: ISO/IEC 27005 Information technology - Security techniques - Information security risk management. ISO 27005: 2008, International Organization for Standardization, Geneva, Switzerland (2008)
16. ISO: ISO/IEC 27001 Information Security Management System (ISMS) standard. ISO 27001: 2013, International Organization for Standardization, Geneva, Switzerland, October 2013
17. ISO: ISO/IEC 27000 Information technology - Security techniques - Information security management systems, Overview and vocabulary. ISO 27000: 2014, International Organization for Standardization, Geneva, Switzerland, May 2014

18. Jin, X., Sandhu, R., Krishnan, R.: RABAC: role-centric attribute-based access control. In: Kotenko, I., Skormin, V. (eds.) MMM-ACNS 2012. LNCS, vol. 7531, pp. 84–96. Springer, Heidelberg (2012). doi:10.1007/978-3-642-33704-8_8
19. Jürjens, J.: Secure information flow for concurrent processes. In: Palamidessi, C. (ed.) CONCUR 2000. LNCS, vol. 1877, p. 395. Springer, Heidelberg (2000)
20. Jürjens, J.: Modelling audit security for smart-card payment schemes with UMLsec. In: 16th International Conference on Information Security (IFIPSEC 2001), pp. 93–108. IFIP, Kluwer (2001)
21. Jürjens, J.: Secure Systems Development with UML. Springer, New York (2005). Chinese translation: Tsinghua University Press, Beijing 2009
22. Jürjens, J.: Verification of low-level crypto-protocol implementations using automated theorem proving. In: 3rd ACM & IEEE International Conference on Formal Methods and Models for Co-Design (MEMOCODE 2005), pp. 89–98. Institute of Electrical and Electronics Engineers (2005)
23. Jürjens, J., Wimmel, G.: Formally testing fail-safety of electronic purse protocols. In: 16th International Conference on Automated Software Engineering (ASE 2001), pp. 408–411. IEEE (2001)
24. Jürjens, J., Wimmel, G.: Security modelling for electronic commerce: the common electronic purse specifications. In: Schmid, B., Stanoevska-Slabeva, K., Tschammer, V. (eds.) Towards the E-Society: E-Commerce, E-Business, and E-Government. IFIP, vol. 74, pp. 489–505. Springer US, New York (2001)
25. National Institute for Standards and Technology: The NIST Definition of Cloud Computing. Technical report, Special Publication 800–145 of the National Institute of Standards and Technology (NIST), September 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
26. Nist, Aroms, E.: NIST Special Publication 800–53 Revision 4 Recommended Security Controls for Federal Information Systems and Organizations. CreateSpace, Paramount, CA (2012). http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
27. Ratiu, D., Feilkas, M., Jürjens, J.: Extracting domain ontologies from domain specific APIs. In: 12th European Conference on Software Maintenance and Reengineering (CSMR 2008), pp. 203–212. IEEE (2008)