Chapter 37
A Pattern-Based and Tool-Supported Risk Analysis Method Compliant to ISO 27001 for Cloud Systems

Azadeh Alebrahim
University of Duisburg-Essen, Germany

Stephan Fassbender
University of Duisburg-Essen, Germany

Denis Hatebur
University of Duisburg-Essen, Germany

Ludger Goeke
ITESYS Inst. f. tech. Sys. GmbH, Germany

Isabelle Côté
ITESYS Inst. f. tech. Sys. GmbH, Germany

ABSTRACT

To benefit from cloud computing and the advantages it offers, obstacles regarding the usage and acceptance of clouds have to be cleared. For cloud providers, one way to obtain customers' confidence is to establish security mechanisms when using clouds. The ISO 27001 standard provides general concepts for establishing information security in an organization. Risk analysis is an essential part in the ISO 27001 standard for achieving information security. This standard, however, contains ambiguous descriptions. In addition, it does not stipulate any method to identify assets, threats, and vulnerabilities. In this paper, the authors present a method for cloud computing systems to perform risk analysis according to the ISO 27001. The authors' structured method is tailored to SMEs. It relies upon patterns to describe context and structure of a cloud computing system, elicit security requirements, identify threats, and select controls, which ease the effort for these activities. The authors' method guides companies through the process of risk analysis in a structured manner. Furthermore, the authors provide a model-based tool for supporting the ISO 27001 standard certification. The authors' tool consists of various plug-ins for conducting different steps of their method.

DOI: 10.4018/978-1-4666-8473-7.ch037

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 5 of 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:

1. Maintaining catalogs of patterns for threats, security requirements, vulnerabilities, and controls.
2. Providing traceability links between different types of pattern catalogs.
3. Use of patterns in nearly all phases of the risk assessment process.
4. 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