2014 47th Hawaii International Conference on System Science

A Taxonomic Perspective on Certification Schemes: Development of a Taxonomy for Cloud Service Certification Criteria

Stephan Schneider, Jens Lansing, Fangjian Gao, Ali Sunyaev
University of Cologne
{schneider, lansing, gao, sunyaev}@wiso.uni-koeln.de

Abstract

Numerous cloud service certifications (CSCs) are emerging in practice. However, in their striving to establish the market standard, CSC initiatives proceed independently, resulting in a disparate collection of CSCs that are predominantly proprietary, based on various standards, and differ in terms of scope, audit process, and underlying certification schemes. Although literature suggests that a certification's design influences its effectiveness, research on CSC design is lacking and there are no commonly agreed structural characteristics of CSCs. Informed by data from 13 expert interviews and 7 cloud computing standards, this paper delineates and structures CSC knowledge by developing a taxonomy for criteria to be assessed in a CSC. The taxonomy consists of 6 dimensions with 28 subordinate characteristics and classifies 328 criteria, thereby building foundations for future research to systematically develop and investigate the efficacy of CSC designs as well as providing a knowledge base for certifiers, cloud providers, and users.

1. Introduction

Cloud computing environments are characterized by uncertainty and lack of transparency [1]. In particular, there is a dearth of guidelines and tools to support potential adopters to comprehensively assess cloud services in terms of individual profitability and risks, such as security and availability. Recent research proposes that such concerns can only partly be alleviated by technical protections such as encryption and should be complemented by (real-time) audits [2]. Similarly, researchers propose certifications based on third-party audits as decision support tools [3]. Certifications can create transparency in the market, increase trust and acceptance of potential adopters, and enable cloud providers to review and improve their systems and processes [4, 5, 6]. This is why the European Union declared developing cloud service certifications (CSCs) a key action of their cloud strategy [7].

As a result, numerous CSC initiatives are emerging (e.g., Cloud Security Alliance STAR, EuroCloud, FedRAMP, TRUSTed Cloud Data Privacy Certification). However, these initiatives are still in an early stage and have potential for improvements [8]. For instance, sourcing decisions involve stakeholders from multiple organizational functions with different information needs [9, 10]. A legal department, for example, has different requirements for cloud services than an IT department or the business unit using a cloud service. Thus, depending on roles and responsibilities, stakeholders put different weights on evaluation criteria and have other information needs [9, 11]. Therefore, a certification scheme should be semantically rich and structurally sound, designed with the purpose to cope with information needs of multiple stakeholders. However, these requirements are only partially reflected in current CSCs' designs.

Despite calls for developing CSCs [5, 7, 12], research on designing CSCs is scarce. Recent research indicates that a certification's design in terms of content (i.e., the certification scheme) influences its effectiveness [13]. Thus, CSCs will only be effective if properly designed in due consideration of the peculiarities of the cloud computing paradigm. Existing cloud standards and CSCs provide profound knowledge on requirements for cloud services and what criteria providers and services need to fulfill. However, this knowledge and the generic structural characteristics of CSC schemes have not been formalized so far. Taxonomies provide a means to delineate and structure knowledge within a field [14] and hence are a promising vehicle to derive a common structure for CSCs. Thus, the objective of this paper is to address the identified research gap at its very foundation and develop a taxonomy for CSC criteria, thereby answering the following research question: *how can CSC criteria be classified?*

To answer the research question, we apply the method of Nickerson et al. [15] and develop a taxonomy for CSC criteria drawing data from 13 expert interviews and 7 cloud standards. The resulting taxonomy contains 328 certification criteria, classified in a taxonomy with 6 dimensions with each between 2 to 9 characteristics.

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.614

IEEE computer society

By developing the taxonomy, we address three key research needs identified in research and practice. First, by "cutting through the jungle of standards" we identify a map of cloud standards for developing CSC schemes [7]. Second, we build foundations for developing (semi-)automated methods to analyze, monitor, and certify cloud services [2, 12, 16]. Third, the taxonomy can serve as a basis for developing structured and machine-readable descriptions of certification schemes and audit reports. Thus enabling automated compliance audits according to predefined metrics [2, 16, 17] as well as allow addressing different stakeholders' information needs through interactive and filterable presentation of CSCs [8].

The remainder of this paper is structured as follows. In section 2, we provide a background on cloud computing and certifications. Section 3 outlines the research approach, followed by the resulting taxonomy in section 4. We conclude with a discussion and provide implications for future research.

2. Background

Cloud computing is an IT sourcing model, based on virtualization that provides on-demand network access to a shared pool of managed and highly scalable IT resources on a pay-per-use basis [18]. The IT resources refer to hardware (Infrastructure as a Service, IaaS), development platforms (Platform as a Service, PaaS), and applications (Software as a Service, SaaS) and "can be rapidly provisioned and released with minimal management effort or service provider interaction" [18]. Despite promising opportunities related to cloud computing [19], numerous adoption success stories [20], and auspicious market predictions [21], there is still a high level of uncertainty concerning the adoption of cloud computing [1]. In this context, certifications of cloud services can mitigate such uncertainties [6].

Certification is defined as a process in which a third party formally confirms that a product, process, or service conforms to a set of predefined criteria (i.e., a certification scheme) [22].

Standardization activities in the field of cloud computing increased in recent years [23], resulting in a proliferation of standards and confusion in terms of which standards serve best for addressing specific issues such as security, availability, or interoperability [7]. In this context, we use the term standard synonymously for guideline, framework, and best practice. Still, standards remain important means to cope with the challenges in cloud computing environments because they assist potential adopters evaluating cloud services and assessing cloud readiness of their own business processes. However, regarding external providers' compliance, users are left to trust a provider that it adheres to specific standards. In contrast, CSCs provide a higher level of assurance, as they require audits by independent and trustworthy third parties. Nevertheless, development of both CSCs and standards is important, because CSCs can gain important inputs from existing standards [4, 24].

Extant research already proposes certifications as a means to assess quality and performance of IT services in procurement processes [3]. In the context of cloud computing, Schneider et al. [8] derived a set of design recommendations for CSCs in an empirical study. These design recommendations constitute a general framing for CSCs. According to Schneider et al. [8], the issuing organization should be an independent and experienced organization with high reputation trusted by (potential) clients (e.g., a standardization body or industry association). The auditing organization should be an accredited organization or industry association and should be detached from the consultant mandate to prepare for the audit in order to prevent courtesy audits. The auditing process should be conducted on site with document reviews and interviews. Additionally, the process should be accompanied by regular re-audits as well as (semi-)automated monitoring to continuously control that a certified service adheres to the CSC's requirements. The underlying certification scheme should be tailored to information needs of multiple stakeholders, publicly available in full detail, deployable as a scheme for third parties to certify cloud services, for cloud providers to conduct a self-assessment of their services, and for cloud users to aid decision support. The certification should certify a single service and not an entire organization and should aim at an internationally agreed legal framework with components at the national or jurisdiction level [8].

With cloud systems becoming more complex and interconnected, resources being obtained and released location independently and on-demand, more sophisticated mechanisms that ensure compliance with certifications are required. Existing CSCs represent only a snapshot and historical assessment of the cloud service, with re-audits every one to three years. However, continuous monitoring of cloud services is necessary in order to provide ongoing reliable and secure cloud services [2]. In this context, Accorsi et al. [16] suggest an automated certification scheme for cloud-based business processes. However, research on automated certification is still in its infancy. Cloud services are highly complex, interconnected systems and many processes behind cloud services are not automatically or only semi-automatically executable, even less automatically certifiable. This is particularly true for small and medium cloud service providers, who have not yet implemented or upgraded their business processes to support the high degree of automation envisioned for cloud services [19]. Moreover, human-driven, partly unstructured interactions increase complexity and complicate the automated certification of compliance requirements for cloud services such as privacy, and data security. However, research has shown that even such complex systems can be certified automatically for compliance [25]. Yet, possible flaws occurring due to system weaknesses might remain unrecognized if users solely rely on automated certification systems [26]. Thus, even though some parts of audits might be automated, human auditors still need to manually evaluate specific aspects of cloud services. Therefore, certification schemes should be classified by type of audit process with which each criterion should be assessed.

3. Research approach

We followed a three-phase approach to develop the taxonomy for CSC criteria. First, we conducted thirteen semi-structured expert interviews to gather expert knowledge as a basis for the taxonomy development process. Next, we followed an iterative method for taxonomy development [15]. We first analyzed interview transcripts to derive dimensions and characteristics for the taxonomy and then derived certification criteria from seven cloud standards. In the last phase, we classified each certification criterion in the taxonomy. In the following, we elaborate on the research approach for each phase in more detail.

3.1. Conducting expert interviews

We conducted thirteen semi-structured expert interviews with practitioners of cloud service providers, cloud service users, and consultants. All companies are located in Germany (German companies or German subsidiaries of international companies). Interviewees were selected aiming at a diverse pool of interviewees to gain insights from different stakeholder perspectives. Hence, we conducted interviews with executives, since they are responsible for strategic IT sourcing decisions and are the main drivers for IT innovations [27]. Heads of IT and middle management were included because they are responsible for evaluating potential solutions [27, 28, 29]. Moreover, we interviewed consultants because they are involved in selecting and implementing cloud services [30]. We also interviewed users from business departments to gain insights from an operational perspective.

Interviewees have an average work experience of 17 years and have worked on an average of 6 projects involving deployment or procurement of cloud services. Of the 13 interviewees, 5 are from top management, 6 from line or project management and 2 are employees. In terms of function, 7 are affiliated with an IT function, and 6 with a business function. Concerning the organizations of the interviewees, 8 provide cloud services and 10 use cloud services. A detailed list of interviewees is depicted in Table 1.

Table 1. Interviewee details

ID	Job title	Organization
i01	Senior Research Manager	Consulting
i02	CEO	Sw. Solutions
i03	Head of Research Department	Consulting
i04	Director Sw. Development	Sw. Solutions
i05	Global Server Virtualization Offering Lead	Consulting
i06	Senior Consultant	Consulting
i07	Cloud Territory Business Manager	Sw. & Hw. Solutions
i08	CEO	IT Services
i09	CEO	Sw. Solutions
i10	CMO	Sw. Solutions
i11	CEO	Sw. Solutions
i12	Innovation Manager	IT Services
i13	Sales Manager	Sw. Solutions

The interview guideline was structured according to two general themes. First, interviewees were asked to reflect on previous cloud sourcing projects. We gathered perceptions on and requirements for CSCs indirectly by asking open questions about the decision process and conducted activities, involved stakeholders and respective responsibilities, selection and evaluation criteria, challenges that occurred during the projects, as well as drivers and inhibitors for cloud sourcing. Second, we asked the interviewees directly about their perceptions of and requirements for CSCs in terms of auditing process, auditor and issuer, as well as scope and certification assurances. As data collection and data analysis overlapped iteratively, we revised the interview guideline throughout the interviews to discuss themes that emerged in prior interviews.

For quality assurance, we discussed the interview guideline with six fellow researchers and then conducted two pilot interviews, which resulted in minor revisions of the guideline. The two validation interviews are not included in the evaluation. Interviews were conducted between June and September 2012. We conducted, coded, and analyzed the interviews iteratively (cf. next section). Interviews were between 35 and 95 minutes in length, with an average of 59 minutes. We recorded and transcribed all interviews and returned the transcripts to the interviewees for communicative validation [31], resulting in minor wording adjustments.

3.2. Developing the taxonomy

A taxonomy structures and organizes knowledge of a specific field [14]. Taxonomies play important roles in research and practice because "the classification of objects helps researchers and practitioners understand and analyze complex domains" [15] and thereby provide "a fundamental mechanism for organizing knowledge" [32]. According to [15], a taxonomy is an artifact that "describes and classifies existing or future objects in a specific domain" (p. 2) and consists of a "set of n dimensions D_i (i=1, …, n) each consisting of k_i ($k_i \geq 2$) mutually exclusive and collectively exhaustive characteristics C_{ij} (j=1, …, k_i) such that each object under consideration has one and only one C_{ij} for each D_i." (p. 5). Formally stated:

$$T = \{D_i, i = 1, \dots, n \mid D_i = \{C_{ij}, j=1, \dots, k_i; k_i \geq 2\}\}$$

Nickerson et al. [15] developed an iterative method for taxonomy development. Due to brevity, we only describe its application and refer to [15] for a detailed description and a step-by-step application in the mobile applications domain.

3.2.1. Meta-characteristic. First, researchers have to define a meta-characteristic and ending conditions for the taxonomy development. "The meta-characteristic is the most comprehensive characteristic that will serve as the basis for the choice of characteristics in the taxonomy" and its choice "should be based on the purpose of the taxonomy." [15] "Each characteristic [of the taxonomy] should be a logical consequence of the meta-characteristic." [15] We select *certification of cloud services* as our meta-characteristic.

3.2.2. Ending conditions. We defined the following objective ending conditions (cf. [15]): (1) all interviews analyzed (n = 13), (2) all selected standards analyzed (n = 7, cf. section 3.2.5), (3) at least one certification criterion is classified under every characteristic of every dimension, (4) no new dimensions or characteristics were added in the last iteration, (5) no dimensions or characteristics were merged or split in the last iteration, (6) every dimension is unique and not repeated, (7) every characteristic is unique within its dimension. As subjective ending conditions, we adopted the conditions of Nickerson et al. [15]: (8) concise, (9) robust, (10) comprehensive, (11) extendible, and (12) explanatory.

3.2.3. Approach. Nickerson et al. [15] distinguish two approaches: inductive (empirical-to-conceptual; favorable if the researchers have little understanding of the domain but significant data about the objects are available) and deductive (conceptual-to-empirical; favorable if little data are available but the researchers have significant understanding of the domain). As we have access to both, extensive data (cloud standards, cf. [23]) and extensive knowledge of the domain (expert interviews and own experience), we choose to start with the deductive approach to derive characteristics and dimensions from the interviews and later conduct inductive iterations to derive the certification criteria (i.e., objects). Table 2 lists the approach and data sources for each iteration.

Table 2. Taxonomy development iterations

Iteration	Approach	Data source
1	deductive	i01, i02, i03
2	deductive	i04, i05, i06
3	deductive	i08, i09, i19, i11
4	inductive	[4]
5	deductive	i07, i12, i33
6	inductive	[33]
7	inductive	[34]
8	inductive	[35, 36]
9	inductive	[37]
10	inductive	[38]

3.2.4. Deductive iterations. We used NVivo software for meaning coding, condensation, and interpretation of interviewees' statements [39]. Two researchers independently analyzed the interviews by iterative, descriptive, and interpretive coding [40] aiming to identify statements to deduce dimensions, characteristics, and objects for the taxonomy. The interviews predominantly influenced deduction of characteristics and dimensions, because the interviewees' statements rarely provided concrete certification criteria. Interviewees rather named generic high-level criteria such as 'location and security of the data center [are important to be certified].' [i07] or 'legal and particularly contractual aspects of a cloud service are explicitly crucial for a certification.' [i10]. Further, interviewees characterized certification criteria by statements such as 'if we are talking about security, […], then the auditor has to be on site in order to assess how the provider manages its security.' [i08] or 'on top of the stack, there is the service, which is based on some hardware at the bottom of the stack. Everything in between, I would slice into layers, because that's where a cloud service provider can obtain services from sub providers, which in turn must fulfill the certification requirements as well.' [i01]. Such statements were used to identify characteristics of the taxonomy. For instance, the statements of i07 and i10 demonstrate three characteristics that are summarized in the dimension *assurance*: *security*, *contract, and legal compliance*. The statement of i08 demonstrates the dimension *on-site audit* (characteristics: *yes*, *no*), and i01's statement demonstrates the dimension *service layer* (characteristics: *utility layer*, *application layer*, *all layers*). Statements that were sufficiently precise, served as objects in the taxonomy, but were marked to be refined in subsequent inductive iterations by detailed and measurable certification criteria extracted from the selected standards. For instance: 'what should definitely be included in the agreement, is that the provider has to inform its customers about occurred incidents that might affect the customers' data.' [i06]. This criterion was refined and enriched in the inductive iterations by criteria concerning incident management extracted from ISO 27001 and ITIL. After the fifth iteration, we met and discussed the taxonomy, which resulted in minor changes. The remaining inductive iterations did not result in changes of the taxonomy.

3.2.5. Inductive iterations. In order to derive the certification criteria, we selected well-known and established standards for cloud computing, IT security, and IT services that have a high maturity level and a high impact potential as assed in [23, 41]. We aimed to select a set of standards that on the one hand collectively covers a broad range of assurances for cloud services as identified in the interviews, and on the other hand provides in-depth knowledge on highly relevant issues such as security and privacy. Therefore, we selected comprehensive standards that covered a broad range of topics in one standard [35, 36], as well as specific standards that focus on one particular topic such as security [4, 33, 34], service management [38], or legal compliance [37]. We derived certification criteria from each standard as follows.

One researcher sequentially read and analyzed the standards to identify eligible certification criteria, extracted suggestions or requirements for cloud services as certification criteria, and rephrased them as questions that can be answered with yes or no. Each extracted criterion was compared to already existing criteria in the taxonomy. Similar criteria of different standards were merged and rephrased, wide-ranging or imprecise criteria that would have to be assigned to multiple characteristics within one dimension were split in smaller, more specific criteria. Since only one researcher conducted this activity, merging criteria was done very cautiously. Only if two criteria were doubtless identical, they were merged in this phase. Otherwise, a new criterion was inserted, and we handled merging of criteria in the next phase.

This approach resulted in a total of 417 certification criteria. After ten iterations, we reached all objective and subjective ending conditions.

3.3. Classifying certification criteria

We conducted this phase in order to reduce subjectivity of the classification and increase validity and reliability of the taxonomy. Only one researcher conducted the inductive iterations, that is, extracting all certification criteria from the standards, merging and rephrasing criteria, and classifying each derived criterion within the taxonomy. Since classification by a single researcher is biased by subjectivity, we discarded all classifications, thus only having the 417 certification criteria and the taxonomy structure (dimensions and characteristics). We then scheduled workshops with four researchers and assigned tasks to each of them in order to classify derived certification criteria, as well as merge and delete obsolete and duplicate criteria. We followed an iterative approach consisting of individual preparation work of each researcher and team based discussions.

First, we selected a random set of 50 criteria. Each researcher individually classified each criterion. We then met and discussed problems that occurred during the classification process as well as conflicting classifications. After discussing and resolving problems, we established a general set of rules for classification. Rules were derived from problems that occurred, for instance, if a researcher was indecisive between two characteristics within one dimension.

Second, we formed teams of two researchers (team 1: researcher A+B, team 2: researcher C+D). Each team met and classified the remaining 367 criteria in sets of 90 criteria per iteration. After having classified 90 criteria, we switched teams: researcher A and C as well as researcher B and D met. These teams then compared and discussed the classifications that were previously classified in the teams with different researcher constellations. After discussing and resolving conflicts, we classified the next batch of 90 criteria. After having classified all criteria and having discussed all conflicts, one researcher screened all criteria for consistency.

The classification of the certification criteria led to reduction of the overall number of criteria from 417 to 328, but did not result in changes of the taxonomy. The seemingly significant reduction by 89 criteria was intended and resulted from the directive in the previous phase that the single researcher should prefer to insert duplicate criteria in the taxonomy rather than merge criteria that are not certainly identical.

4. Results

Table 3 depicts the developed taxonomy with 28 characteristics in 6 dimensions as well as lists the total number and relative share of objects classified within the dimension for each characteristic.

The dimension *assurance* describes the objective that shall be achieved by certifying a criterion. This dimension allows cloud service users to evaluate a certified cloud service in terms of non-functional requirements. Existing CSCs are often structured along (a subset of) the characteristics of this dimension (e.g., [24]). The dimension *on-site audit* describes whether or not an auditor has to be on site in order to assess a criterion. The *primary method* characterizes how a criterion shall be assessed and *continuous monitoring* states whether or not a criterion needs be monitored by a third party during operation. The *service layer* describes which layer has to be certified in order to confirm a criterion. As cloud services can be deployed as a cascade of infrastructure, platform, and software services, some criteria only have to be fulfilled from the infrastructure provider (e.g., data center security). If a SaaS provider utilizes IaaS services, the criteria of the utility layer need to be certified at the IaaS provider. We follow Armbrust et al. [19] and subsume PaaS and IaaS in the utility layer, as the 'distinction between PaaS and IaaS is not crisp and the two are more alike than different.', in particular in terms of certification criteria. The *focal entity* describes what kind of entity is assessed in order to certify a criterion, for instance, a process, a contract, or a software.

Since we cannot provide and describe the classification of each of the 328 certification criteria due to page restrictions, we provide two classification examples below (the complete certification scheme with all 328 certification criteria classified within the taxonomy is available from the authors on request).

Example criterion 1: 'Are all major supply components for the data center such as electricity, air conditioning, Internet access, and cabling implemented redundantly?' This criterion has the objective to *assure availability* by conducting an *on-site asset review without continuous monitoring* of the *infrastructure* that supplies the *utility layer* of a cloud service**.**

Example criterion 2: 'Is the cloud provider equipped with the necessary tools to recover the cloud service in an event of damage or loss?' This criterion has the objective to *assure availability* by conducting *on-site interviews* with technical personal *without continuous monitoring* about the *processes* in place to recover cloud services of *all layers***.**

These two examples illustrate how we classified the criteria. Our goal was to evaluate each criterion with regard to the most appropriate classification. For instance, interviewing employees about the implementation of a process usually also includes reviewing the process documentation. However, as in the second example, interviews are the auditor's primary data source, we classified 'interview' as the primary audit method for this criterion.

Table 3. Taxonomy of CSC criteria

Dimension	Characteristic	#	%
Assurance	Security	179	55%
	Privacy	24	7%
	Legal Compliance	12	4%
	Flexibility	3	1%
	Interoperability	7	2%
	Availability	45	14%
	Financial Stability	1	0%
	Customer Support	15	5%
	Contract	42	13%
On-Site Audit	Yes	203	62%
	No	125	38%
Primary Method	Interview	90	27%
	Service Usage	12	4%
	Asset Review	115	35%
	Document Review	108	33%
	Automatic Audit	3	1%
Continuous Monitoring	Yes	37	11%
	No	291	89%
Service Layer	Utility Layer	82	25%
	Application Layer	65	20%
	All Layers	181	55%
Focal Entity	Process	137	42%
	Provider	4	1%
	Service	22	7%
	Infrastructure	28	9%
	Software	77	23%
	Contract	52	16%
	Employee	8	2%

5. Discussion

We derived a taxonomy for CSC criteria by applying the method of Nickerson et al. [15]. After ten iterations, we reached all objective and subjective ending conditions. In order to evaluate the usefulness of our taxonomy as well as the applicability of the method, we first discuss the applied subjective ending conditions and then discuss our results.

5.1. Subjective ending conditions

Conciseness. According to Nickerson et al. [15], the number of dimensions and characteristics should be assessed by comparing them with the maximum amount of input information suggested by research on cognitive capacity in decision making, for instance, seven plus or minus two [42]. In this context, our taxonomy is concise with six dimensions and between two and nine characteristics per dimension.

Robustness. "A useful taxonomy should contain enough dimensions and characteristics to clearly differentiate the objects of interest." [15]. With 6 dimensions and 28 characteristics, we defined and delineated each dimension and characteristic as a distinct attribute of a certification criterion and thereby the taxonomy proves robust in differentiating among objects. The efficiency of our taxonomy to differentiate between objects across multiple dimensions might be illustrated as follows. In the first place, we identified the characteristic *process maturity* in the dimension *assurance*. However, process maturity is rather an underlying assurance that enables other assurances such as security and availability. Additionally, having the characteristic *process* in the dimension *focal entity* makes the characteristic *process maturity* in the *assurance* dimension redundant. Thus, process maturity is covered in the taxonomy by criteria that have a *process* as *focal entity* with the *assurance* depending on the purpose of the process, for instance, *security*. Thus, allowing a rich description and differentiation of objects within the taxonomy.

Comprehensiveness. A taxonomy should be comprehensive in terms of completeness and complete descriptions. Completeness refers to the requirement that the taxonomy "can classify all known objects within the domain under considerations." [15]. Complete descriptions means that the taxonomy "includes all dimensions of objects of interest." [15].

In terms of completeness, the selection of only 7 standards is a limitation of our work. Including further standards such as COBIT, CMMI, or SOC 3 will result in new certification criteria. However, based on the number of already classified criteria (328), we are certain that criteria, which could be extracted by analyzing more standards, can be classified in the taxonomy as well. Furthermore, as we aimed at selecting standards that are widely accepted, from different institutions with varying focus (cf. section 3.2.5), we are confident that the most important criteria are covered by our certification scheme. In this context, the ratio of the number of newly added criteria and the number of criteria merged with existing criteria (i.e., two standards contain two similar or identical criteria), decreased with each inductive iteration, which indicates a saturation of covered certification criteria.

In terms of complete descriptions, the limited number of 13 expert interviews is a limitation of our work as well. However, we aimed at gathering a broad knowledge base by interviewing experts on different levels, with varying roles from providers, users, and consultants. No new characteristics or dimensions were added to our taxonomy after the fifth iteration, meaning that we extracted and classified criteria from six standards without being able to identify new characteristics or dimensions. Since the standards cover a broad range of topics, we are confident that our interview partners provided a comprehensive knowledge base for taxonomy development. Therefore, we conclude that our taxonomy is comprehensive.

Extendible. "A useful taxonomy should allow for inclusion of additional dimensions and new characteristics within a dimension when new types of objects appear." [15]. This condition is met. For example, if new service models would appear that require specific certification criteria, characteristics could be added to the dimension *service layer.*

Explanatory. The last ending condition assesses what dimensions and characteristics explain about an object. The explanatory value of the taxonomy is best illustrated by the fundamental question each dimension answers about a certification criterion. *Assurance*: why has a cloud service to fulfill this criterion? This dimension allows cloud service users to evaluate a certified cloud service in terms of non-functional requirements. *On-site*: where is the audit conducted? *Primary method*: how is the audit conducted? *Continuous monitoring*: is ongoing monitoring required? *Service layer*: which layer has to be certified (in terms of who provides the respective layer for the cloud service)? *Focal entity*: what is audited?

In summary, the taxonomy can be considered as useful (cf. [15]). At the same time, by developing a useful taxonomy with the method of Nickerson et al. [15], we illustrate and provide further evidence for the applicability of their method.

5.2. Taxonomy and classification

Taking a look at the distribution of objects within each dimension unveils that the objects are unevenly distributed over characteristics. For instance, it is apparent that most objects are classified as security (179) or availability (45) assurances, whereas only 1 object is classified as financial stability assurance and only 3 as flexibility assurances. Furthermore, 42% of the criteria are classified to assess a process as focal entity. We identified three possible reasons for this unequal distribution. First, the distribution might reflect the importance of assurances to cloud service users as identified in previous research on CSCs [8, 43] as well as research on risks in the cloud computing context [19, 44]. In our interviews, financial stability was discouraged to be included in a certification by four out of eight participants and only one participant favored flexibility to be included in a certification. Second, the distribution could be a result of standards selection, since three out of seven standards are security focused. With ISO 27001 and ITIL we also included two standards that have a strong emphasize on aligning processes within an organization. None of the standards focused on providers' financial stability, but rather addressed this assurance as a sideline. Third, the characteristics differ in terms of granularity. Assessing a cloud provider's financial stability could be broken down to a few metrics that aim at ensuring business continuity of the provider. However, assessing a cloud provider's security requires a much more granular assessment such as data security, network security, data integrity, data segregation, data locality, data access, authentication and authorization, and more [45]. Maybe, including other standards not originating from the IT domain might bring up more objects classified as financial stability assurance.

Concerning completeness of the taxonomy in terms of complete description, one could argue that additional dimensions should be included in the taxonomy. For instance, after the first iteration, our taxonomy included the dimensions *industry* (potential characteristics could be derived from [46]), *region* (characteristics: jurisdictions such as EU, US, etc.), and *stakeholder relevance* (characteristics: *technical*, *functional*, *economic*, *legal*). However, including these dimensions and characteristics would violate the mutual exclusive restriction (no object can have two different characteristics in a dimension), since most criteria are applicable in multiple industries, jurisdictions, or relevant to multiple stakeholders. Building permutations in order to fulfill the mutual exclusive restriction would violate the subjective ending condition for the taxonomy to be concise. Therefore, we decided to develop a generic certification scheme in the first place, including all identified certification criteria. In order to build industry-specific, jurisdiction-specific, or stakeholder-specific certification schemes, further research is necessary. However, these specific certifications schemes can be realized by mapping certification criteria. Thus, industries, jurisdictions, or stakeholder groups just need to identify relevant subsets of the 328 criteria. However, further research is necessary to identify these subsets.

Furthermore, if the taxonomy shall be deployed for use in marketplaces as service description, the taxonomy needs to be extended to include, for example, functional aspects (e.g., [47, 48]).

Our classification reveals potential for future research on (semi-)automated methods for auditing and monitoring cloud services. We could only identify 3 criteria that can be certified automatically, but identified 37 criteria (11%) that require continuous monitoring. For instance, 108 criteria (33%) were classified as document review for primary audit method. Supporting such reviews by automated document or log data analysis (e.g., [17]) can reduce human effort and thereby costs for the certification and enable continuous monitoring of cloud services.

6. Conclusion

In this paper, we developed a taxonomy for CSC criteria. The resulting taxonomy contains 6 dimensions with each between 2 and 9 characteristics. This paper contributes to research and practice. In terms of research, our study provides three principal contributions.

First, we contribute to cloud computing research by providing a systematically derived structure of CSC characteristics which can be used as a device to structure and organize knowledge in the field of cloud computing and CSC, for example, to organize cloud standards or to develop and structure certification schemes (cf. [7]). A map of cloud standards could be aligned to the dimensions and characteristics of our taxonomy, for instance, standards supporting to achieve a specific assurance (e.g., security), standards for auditing methods (e.g., semi-automated document reviews), standards enabling continuous monitoring of cloud services (e.g., automated vulnerability checks), standards relevant for a particular service layer (e.g., utility layer), or standards for specific entities (e.g., software architecture for cloud services). Similarly, research can be aligned according to the taxonomy. By outlining potential for industries, jurisdictions, or stakeholder groups, the taxonomy also provides a basis for future research on quality assurances specific to particular target groups. Researchers may also build on the taxonomy when developing similar taxonomies for certifications in different domains (e.g., health care).

Second, we apply a recently developed artifact (i.e., a method for taxonomy development) to build a new artifact (i.e., a taxonomy for CSC criteria). Thereby, we add to the body of design science research by evaluating an existing artifact in a novel domain and by building a new artifact. Our taxonomy supports design science researchers in developing cloud-specific artifacts, such as certification schemes, service descriptions, or auditing methods. Since we only built the taxonomy and did not evaluate it in a real-world certification context, the taxonomy is subject to further evaluation. In future research, we will evaluate the taxonomy by discussing it with accredited and experienced auditors (e.g., ISO 27001 auditors) as well as multiple stakeholder groups in order to derive stakeholder group specific schemes. We will further conduct workshops with legal experts as this stakeholder group is missing in our interviews.

Third, we add to the knowledge on CSC by identifying certification criteria that require continuous monitoring of adherence to certification requirements. Thereby, we provide a starting point for future research on development of (semi-)automatic methods to analyzing, monitoring, and certifying cloud services (cf. [2, 12]).

Contribution to practice is twofold. First, we derive a certification scheme for cloud services consisting of a set of basic certification criteria that constitute a common denominator for high quality cloud services, thereby supporting cloud certification providers, cloud service providers, and cloud service users. Cloud certification providers can assess their CSCs against the taxonomy and the set of identified certification criteria in order to enhance the comprehensibility of their own certification scheme. Cloud service providers can use the certification scheme for a self-assessment of their services and to improve their services accordingly. (Potential) cloud service users can use the certification scheme as a structured requirements guideline to assess cloud services and establish knowledge on what to consider when reviewing a CSC.

Second, the taxonomy of certification criteria serves as a basis for implementing semantically rich and structurally sound machine-readable descriptions of cloud services and certification reports. Machine-readable descriptions are beneficial for three purposes. First, they allow to present interactive and filterable audit reports that are quickly comprehensible and capable of satisfying different stakeholders' information needs [8]. Furthermore, machine-readable descriptions provide a basis for online marketplaces and cloud service review websites to systematically structure, describe, and compare cloud services [48]. Last, machine-readable descriptions enable automated service discovery and selection, in particular for general-purpose services such as IaaS: cloud service users can use the taxonomy to specify minimum requirements for cloud services in (i.e., the minimum set of criteria to be fulfilled) and match these requirements with certification reports or service descriptions of cloud services that adhere to the taxonomy, thereby easing discovery and selection of cloud services.

Despite the contributions and outlined benefits of CSCs, there are still challenges to be addressed. For instance, the willingness of cloud providers to accept and undergo CSCs or the difficulty of implementing continuous monitoring and real-time audits in a secure manner without significantly impairing performance and profitability (cf. [6] for a discussion of CSC challenges).

7. References

[1] http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf 2011.

[2] Juels, A., and Oprea, A., "New Approaches to Security and Availability for Cloud Data", Communications of the ACM, 56(2), 2013, pp. 64-73.

[3] Praeg, C.-P., and Schnabel, U., "It-Service Cachet - Managing It-Service Performance and It-Service Quality", 39th Hawaii International Conference on System Sciences, 2006.

[4] http://bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Minimum_information/SecurityRecommendationsCloudComputingProviders.pdf 2011.

[5] Khan, K.M., and Malluhi, Q., "Establishing Trust in Cloud Computing", IT Professional, 12(5), 2010, pp. 20–27.

[6] Sunyaev, A., and Schneider, S., "Cloud Services Certification", Commun. of the ACM, 56(2), 2013, pp. 33-36.

[7] http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf 2012.

[8] Schneider, S., Lansing, J., and Sunyaev, A., "Empfehlungen Zur Gestaltung Von Cloud-Service-Zertifizierungen", Industrie Management, 4, 2013, pp. 13–17.

[9] Narayandas, D., "Building Loyalty in Business Markets", Harvard Business Review, 83(9), 2005, pp. 131-139.

[10] Mohan, K., Xu, P., and Ramesh, B., "Supporting Dynamic Group Decision and Negotiation Processes: A Traceability Augmented Peer-to-Peer Network Approach", Information & Management, 43(5), 2006, pp. 650-662.

[11] De Looff, L.A., "Information Systems Outsourcing Decision Making: A Framework Organizational Theories and Case Studies", Journal of Information Technology, 10(4), 1995, pp. 281-297.

[12] http://www.bmbf.de/foerderungen/18899.php 2012.

[13] Kim, D., and Benbasat, I., "Trust-Assuring Arguments in B2c E-Commerce: Impact of Content, Source, and Price on Trust", Journal of Management Information Systems, 26(3), 2009, pp. 175-206.

[14] Glass, R., L., "Contemporary Application-Domain Taxonomies", 12(4), 1995, pp. 63–76.

[15] Nickerson, R.C., Varshney, U., and Muntermann, J., "A Method for Taxonomy Development and Its Application in Information Systems", European Journal of Information Systems, 2012.

[16] Accorsi, R., Lowis, L., and Sato, Y., "Automated Certification for Compliant Cloud-Based Business Processes", Business & Information Systems Engineering, 3(3), 2011, pp. 145-154.

[17] Accorsi, R., and Stocker, T., "Automated Privacy Audits Based on Pruning of Log Data", 12th Enterprise Distributed Object Computing Conference Workshops, 2008, pp. 175-182.

[18] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf 2011.

[19] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., and Zaharia, M., "A View of Cloud Computing", Communications of the ACM, 53(4), 2010, pp. 50-58.

[20] Narasimhan, B., and Nichols, R., "State of Cloud Applications and Platforms: The Cloud Adopters' View", Computer, 44(3), 2011, pp. 24-28.

[21] http://www.gartner.com/it/page.jsp?id=2163616 2012.

[22] Iso/Iec, Conformity Assessment — Vocabulary and General Principles 2004.

[23] http://www.bmwi.de/English/Redaktion/Pdf/normungs-und-standardisierungsumfeld-von-cloud-computing 2012.

[24] http://www.saas-audit.de 2011.

[25] Doganata, Y., and Curbera, F., "Effect of Using Automated Auditing Tools on Detecting Compliance Failures in Unmanaged Processes", International Conference Business Process Management, 2009, pp. 310−326.

[26] Mercuri, R.T., "On Auditing Audit Trails", Communications of the ACM, 46(1), 2003, pp. 17-20.

[27] Dibbern, J., Goles, T., Hirschheim, R., and Jayatilaka, B., "Information Systems Outsourcing: A Survey and Analysis of the Literature", The DATA BASE for Advances in Information Systems, 35(4), 2004, pp. 6–102.

[28] Kern, T., Kreijger, J., and Willcocks, L., "Exploring Asp as Sourcing Strategy: Theoretical Perspectives, Propositions for Practice", The Journal of Strategic Information Systems, 11(2), 2002, pp. 153-177.

[29] Willcocks, L., and Fitzgerald, G., "Market as Opportunity? Case Studies in Outsourcing Information Technology and Services", The Journal of Strategic Information Systems, 2(3), 1993, pp. 223–242.

[30] Leimeister, S., Riedl, C., BöHm, M., and Krcmar, H., "The Business Perspective of Cloud Computing: Actors, Roles, and Value Networks", 18th European Conference on Information Systems, 2010.

[31] Flick, U., An Introduction to Qualitative Research, Sage Publications, 4 edn, Los Angeles, 2009.

[32] Wand, Y., Monarchi, D.E., Parsons, J., and Woo, C.C., "Theoretical Foundations for Conceptual Modelling in Information Systems Development", Decision Support Systems, 15(4), 1995, pp. 285-304.

[33] International Organization for Standardization, Iso/Iec 27001:2005: Information Technology -- Security Techniques -- Information Security Management Systems -- Requirements, 2005.

[34] https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf 2011.

[35] http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf 2012.

[36] http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf 2010.

[37] http://en.eurocloud.de/2011/03/04/eurocloud-guidelines-cloud-computing-german-law-data-protection-and-compliance/ 2011.

[38] Stein, F., Schneider, S., and Sunyaev, A., "Itil Als Grundlage Zur Zertifizierung Von Cloud-Services Und -Anbietern", HMD - Praxis der Wirtschaftsinformatik 288, 2012, pp. 33-41.

[39] Kvale, S., Doing Interviews, Sage Publications, Los Angeles, 2007.

[40] Myers, M.D., Qualitative Research in Business and Management, SAGE, Los Angeles, 2013.

[41] Gao, F., and Schneider, S., "Cloud-Frameworks: Eine Übersicht Aus Der Wirtschaftsinformatik-Perspektive", ConLife Academic Conference 2012, 2012, pp. 1-16.

[42] Miller, G.A., "The Magic Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information", Psychological Review, 101(2), 1956, pp. 343-352.

[43] Lansing, J., Schneider, S., and Sunyaev, A., "Cloud Service Certifications: Measuring Consumers' Preferences for Assurances", 21st European Conference on Information Systems, 2013.

[44] Browning, J.A., and Macdonald, N., Survey Analysis: North American Midsize Businesses Cite Cloud Intentions, Gartner Research, 2011.

[45] Subashini, S., and Kavitha, V., "A Survey on Security Issues in Service Delivery Models of Cloud Computing", Journal of Network and Computer Applications, 34(1), 2011, pp. 1-11.

[46] http://www.osha.gov/pls/imis/sic_manual.html 1930.

[47] http://cloudtaxonomy.opencrowd.com/ 2013.

[48] Oberle, D., Barros, A., Kylau, U., and Heinzl, S., "A Unified Description Language for Human to Automated Services", Information Systems, 38(1), 2013, pp. 155-181.