A Taxonomy of IS Certification's Characteristics

Maximilian Renner
Karlsruhe Institute of Technology,
76131 Karlsruhe, Germany
maximilian.renner@kit.edu

Sebastian Lins
Karlsruhe Institute of Technology,
76131 Karlsruhe Germany
lins@kit.edu

Ali Sunyaev
Karlsruhe Institute of Technology,
76131 Karlsruhe, Germany
sunyaev@kit.edu

ABSTRACT

Information system (IS) certifications are considered as a powerful tool for improving the security and trustworthiness of an IS. However, organizations struggle to evaluate and finally adopt appropriate IS certifications. To enhance our understanding of the evaluation of IS certifications, we iteratively develop a taxonomy of key characteristics of IS certifications using inductive and deductive approaches, including expert surveys and interviews. Our taxonomy consists of 17 subjective and objective dimensions, comprising 46 characteristics of IS certifications. Our taxonomy highlights interesting insights into the key characteristics of IS certifications, such as certification targets, scopes, and pricing models, among others, that organizations should consider throughout evaluation. We provide a more fine-grained perspective on IS certifications, guiding future research assessing certification adoption and effectiveness, and supporting organizations in selecting appropriate IS certifications.

CCS CONCEPTS

• **Security and privacy**; • **Systems security**; • **Software and application security**; • **Information systems**; • **Information systems applications**; • **Human and societal aspects of security and privacy**; • **Privacy protections**; • **Social and professional topics**; • **Professional topics**; • **Management of computing and information systems**;

KEYWORDS

IS Certification, Web Assurance Seal, Security, Privacy, Trust, Taxonomy

ACM Reference Format:
Maximilian Renner, Sebastian Lins, and Ali Sunyaev. 2021. A Taxonomy of IS Certification's Characteristics. In *2021 2nd International Conference on Internet and E-Business (ICIEB'21), June 09–11, 2021, Barcelona, Spain.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3471988.3471989

1 INTRODUCTION

Web assurance services and third-party assessments such as information system (IS) certifications and related web seals are considered as powerful tools to improve the security of an IS, signal higher quality of digital platforms, and reduce consumers' uncertainty when using the IS (e.g., regarding the handling of consumer's data) [1-3]. IS certifications are voluntary attestations of specific system characteristics, operations, and management principles by an independent third party regarding security, privacy, and business integrity requirements [1, 2]. Given IS certifications' potential to achieve organizational learning and improvements, and to use them as trust-building tools, IS certifications have become increasingly relevant for organizations operating IS (e.g., cloud services, digital platforms, webshops etc.) and their respective consumers. The well-known certification *"ISO 9001"* for quality management, for example, helps organizations to internalize the actual practices contained in the standard and making changes in organizational quality practices [3]. The importance of IS certifications is also highlighted by the growing adoption rates in electronic markets [4], for example, the major European seal authority TrustedShops has currently issued more than 20,000 web seals to websites to strengthen these websites' trustworthiness. Especially well-known IS certifications, such as "*Certified Privacy*" for webshops, "*CSA STAR*" for cloud services, and the security management standard "*ISO/IEC 27001*", have gained much attention among scholars and practitioners alike [5-7].

The growing importance and diffusion of IS certifications have also their downside. Organizations struggle to evaluate and finally adopt appropriate IS certifications to address prevalent consumer uncertainty or achieve internal improvements due to the sheer amount of potential certifications [1, 2]. By evaluating IS certifications, we refer to the comparison of available IS certifications and selecting a suitable one to satisfy an organization's specific use case and their needs (e.g., specific consumer uncertainty to be resolved). Afterward, organizations adopt the IS certification by internalizing the proposed best practices and undergoing the third-party attestation process. The evaluation of IS certifications is further hampered by IS certification's complexity and outcomes that are challenging to predict in advance. In particular, organizations are concerned whether the intended effects of an IS certification will be achieved (e.g., increasing consumers' willingness to use the system) [3]. Likewise, IS certifications might bundle diverse assurances (e.g., security, privacy, and integrity assurances) to help organizations matching consumers' expectations or internal needs [8]. This bundling makes it even more difficult for organizations to select suitable assurance bundles and predict the impact of certifications [8]. Evaluating and adopting the best fitting certification gains high importance because, for example, if the assurances of certification do not fit the consumers' expectations, they reject the certification altogether, thus rendering the high efforts and costs of organizations to acquire and maintain the certification useless [8].

ICIEB'21, June 09–11, 2021, Barcelona, Spain
© 2021 Association for Computing Machinery.
ACM ISBN 978-1-4503-9021-7/21/06…$15.00
https://doi.org/10.1145/3471988.3471989

Prior research has extensively analyzed why organizations adopt certifications (e.g., to communicate unobservable information about the qualities of an IS) [3, 9, 10]. However, prior research mostly focuses on the adoption process itself, how to achieve benefits of adoption, or analyses a single certification (e.g., "*ISO 9001"* for quality management systems) [11-13]. Consequently, we still lack the knowledge of how to guide organizations in evaluating an appropriate certification for their use case before adoption. Resolving this gap is becoming increasingly important in light of novel certifications and related web seals proving regulatory compliance that are currently under development, such as data protection certifications to prove GDPR compliance (e.g., *AUDITOR* for cloud services) [2, 3, 13]. We want to support organizations to cut through the jungle of IS certifications by thorough evaluation before adoption, and thus seek to answer the following research question (RQ):

RQ: *How can organizations evaluate IS certifications?*

To answer the research question, we identify the key characteristics of certifications in the IS use context impacting organizations' decisions when evaluating IS certifications. To identify the key characteristics, we classified the characteristics of IS certifications by developing a taxonomy according to the approach of Nickerson et al. [14]. We performed deductive and inductive iterations, comprising a survey among organizations, certification authorities, and consumers; diverse interviews with organizations and consumers; discussion workshops with certification researchers; and classifications of existing certifications. The resulting taxonomy contains 17 dimensions and 46 relating characteristics, covering key objective characteristics (e.g., certification target and scope) and subjective characteristics (e.g., reputation and diffusion).

With this study, we advance research by developing means to evaluate multiple IS certifications, which was mostly overlooked in extant research. While prior research only analyzes the impact of certifications from a black box perspective (i.e., adopted vs. not adopted a certification), we also provide a more fine-grained perspective on IS certifications including external trust-building effects and internal improvements of management processes. In doing so, we guide future research to evaluate the introduction and effectiveness of certifications. For organizations, we provide a classification of dimensions and key characteristics that enable comparing several IS certifications and selecting the most suitable ones for organizations' specific needs.

2 THEORETICAL BACKGROUND

2.1 Certification for Information Systems

An IS certification is defined as a voluntary assessment of an organization's IS and related management processes conducted by an independent third party–the certification authority–based on certification criteria (e.g., proprietary catalogues, standards, or regulations) [1][1]. The reasons for organizations to adopt IS certifications are diverse, given external and internal driving forces. Internal driving forces refer to when certifications are adopted autonomously, and organizations benefit by implementing best practices contained in the certification and feedback gained from the third-party assessment, such as improvement of management process or minimization of costs associated with improved internal efficiency. External driving forces refer to the adoption of certifications in response to certain external pressures (e.g., from competitors, consumers, or the government) or incentives, such as increasing consumers' trust in the system by displaying an assurance seal as a graphical representation of the certification on the website or system interface. For example, organizations can use certifications to provide evidence on fulfilling security and data protection by design requirements.

While a wide variety of IS certifications have already been proposed, prior research focuses on three structural elements: (1) content (i.e., the implied assurances), (2) source (i.e., the issuing and auditing authority), as well as (3) process (i.e., the type of attestation process) [1, 3]. Regarding the content, IS certification can be typically divided into three different types addressing (1) privacy, (2) security, and (3) business-integrity concerns of consumers [3]. First, certifications addressing consumers' privacy concerns are used to alleviate consumers' perceived risks in terms of, for example, inappropriate usage of personal data. Second, certifications addressing consumers' security concerns (e.g., unauthorized access, malicious programs, or malware) are used to reassure consumers that an organization uses, for example, intrusion detection software, firewalls, or antivirus, and anti-spyware. Finally, certifications addressing business integrity guarantee fair business practices and reliable management processes (e.g., reliable system administration).

Because IS certifications convey the image that the behavior of an organization and its use context conform to high standards [15, 16], they are becoming increasingly adopted and demanded, leading to the development of further IS certifications. For example, the most recent EU directive on the GDPR stipulates that voluntary data protection certification should be used as the primary means of signaling compliance with the GDPR requirements [16]. Likewise, the novel EU Cybersecurity Act establishes an EU-wide cybersecurity certification framework for digital products, services, and processes, leading to the harmonization of existing and the emergence of novel IS certifications relating to cybersecurity (e.g., ENISA's "*Cybersecurity Certification Scheme on Cloud Services"* (EUCS)). As a consequence, the IS certification market will experience further growth and organizations will face an unforeseen number of available IS certifications. Selecting and adopting an appropriate IS certification to meet external and internal driving forces will, therefore, become even more challenging in the future.

2.2 Related Research

Related research on certifications and related web seals is ever-increasing throughout the recent decades and can be divided into three major streams: (1) developing, designing and innovating certifications and underlying attestation processes, (2) analyzing certifications' impact on consumers; or (3) understanding organizations' rationales for adopting certifications and materializing anticipated

[1] While the breadth of research on certifications has led to varying terminology (e.g., web seals, assurance services, certifications), we follow recent conceptualizations of certifications in the IS discipline [e.g., 1, 2] that attest qualities of IS (e.g., security, privacy and data protection) and related management practices.

Table 1: Overview of related work in the context of adoption and evaluation of certifications.

		Certification research streams	
		Adoption	**Evaluation**
Considerations of certifications	**Single Certification**	A Typical research focus: Motivating forces driving organizations to adopt an ISO 9001 certification Exemplary Studies: [13, 23, 24]	B Typical research focus: Motivators and demotivators impacting organization when evaluating an ISO 9001 certification Exemplary Studies: [11, 25, 26]
	Multiple Certifications	C Typical research focus: Benefits for an organization when adopting ISO 9001 or 140001 certifications Exemplary Studies: [12, 27, 28]	D Typical research focus: Characteristics impacting organizations when evaluating multiple IS certifications Exemplary Study: This study

benefits [17]. First, various scholars have examined the development of trustworthy certifications (e.g., for cloud services [18]), the structural elements of certifications [1], and the increase of certification reliability by performing continuous compliance attestations [19, 20], among others. Second, research taking a consumer perspective seeks to explain how IS certifications affect consumers, why these effects occur and how to predict the effect of certifications on consumers [e.g., 8, 9, 21]. Consumer-related studies have primarily focused on three effects of IS certifications, namely, increasing consumers' trust perceptions, purchase intentions, and perceived assurance [3]. Finally, research taking an organization perspective–which this study aims to contribute to–analyzes the motivations of organizations to adopt certifications and whether organizations can utilize the benefits of adoption, such as improved performance or increased sales [e.g., 11, 22].

Reviewing the literature on evaluating and adopting certifications and related web seals reveals that most studies focus on how to adopt a single (IS) certification, whereas prior literature has mostly neglected to understand how to evaluate multiple certifications. Table 1 separates related work based on their consideration of certifications (analyzing a single certification or several certifications) and their focus on adoption or evaluation of certifications. Quadrant A shows that most of the related work examines internal and external forces that drive organizations to adopt a particular certification (e.g., *ISO 9001*) [e.g., 13, 23, 24]. Quadrant B shows that researchers have also started to identify the motivators and demotivators impacting organizations when evaluating a specific certification before adoption (e.g., *ISO 14001*) [e.g., 11, 25, 26]. As Quadrant C shows, taking a perspective of multiple certifications, research recently compared the benefits of adopting different certifications (e.g., *ISO 9001 and ISO 14001*) [e.g., 12, 27, 28]. Even though prior research provides valuable contributions in adopting and evaluating certifications, prior literature has neglected the evaluation of multiple certifications. In this study, we want to address this gap by developing a taxonomy of key characteristics of certifications in an IS use context that impact organizations' decisions when evaluating IS certifications (Quadrant D).

3 RESEARCH APPROACH

3.1 Developing the Taxonomy

We develop a taxonomy to establish a classification scheme for IS certifications. A classification can be seen as the result of putting objects into groupings or categories [14], whereas a classification scheme is the underlying abstract template. The classification of objects helps researchers and practitioners to understand and analyze complex domains [14]. By establishing a research method to organize knowledge, a taxonomy provides a fundamental mechanism for researchers to describe and classify existing or future objects in a specific domain.

A taxonomy is defined as 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 [14]. More formally, a taxonomy is:

$$T = \left\{D_i, i = 1, \ldots, n | D_i = \left\{C_{ij}, j = 1, \ldots, k_i; k_i \geq 2\right\}\right\}$$

According to this definition, taxonomies' characteristics must be exhaustive and mutually exclusive, with each observed object fulfilling exactly one characteristic in each dimension. To develop the taxonomy, we iteratively apply the research method proposed by Nickerson et al. [14]. First, we define a meta-characteristic for the basis of the taxonomy. Second, we define ending conditions for the determination of the iterations. Third, we iteratively apply two possible approaches to fill the taxonomy with information. On the one hand, we followed an empirical-to-conceptual approach (inductive), which is favorable if significant data about the objects is available [14]. On the other hand, we applied a conceptual-to-empirical approach (deductive) because we have a significant understanding of the domain. We applied a combination of inductive and deductive iterations until the ending conditions were met.

3.2 Meta-Characteristic and Ending Conditions

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 [14]. Each characteristic (of the taxonomy) should be a logical consequence of the meta-characteristic. Drawing on our research question, we define our meta-characteristic to be *key characteristics of certifications in the IS use context impacting organizations' decisions when evaluating IS certifications.*

Due to the research method's iterative nature, predefine conditions to terminate the process must be established. These conditions are both objective and subjective. We evaluated five subjective ending conditions after finishing each iteration: the taxonomy should be (1) concise, (2) robust, (3) comprehensive, (4) extendible, and (5) explanatory. Considering that personal perceptions influence these subjective end conditions, additional eight objective end conditions were assessed after each iteration, which enable an unbiased decision on whether the iterative development process should be terminated [14]: (1) all objects should be examined, (2) no object was merged or split into multiple objects, (3) at least one object is classified under every characteristic of every dimension, (4) no new dimensions or characteristics were added, (5) also no dimension or characteristic were merged or split, (6) the uniqueness of every dimension without any duplication, (7) the uniqueness of every characteristic within its dimension without any duplication, and finally (8) the uniqueness of each cell (the combination of characteristics) without any duplication.

3.3 Iterations to Build the Taxonomy

Since we have access to both extensive data and extensive knowledge of the domain, we decided to start with the deductive approach to derive characteristics and dimensions of IS certifications as initial taxonomy.

For the first iteration, we followed the deductive approach by conducting an online survey with 60 experts representing three different roles: 15 organizations, 24 certification authorities, and 21 consumers. In the survey, we briefly introduced our study's objectives and IS certifications, and then asked participants to describe up to 10 key characteristics of IS certifications. We used content analysis for the conceptualization of characteristics and dimensions [29] while building the initial taxonomy with 15 dimensions and 30 characteristics. To guarantee the content analysis's reliability, two researchers analyzed the survey responses iteratively, achieving a Krippendorff's $\propto$ of 0.65 in the first round and 0.95 in the second round [29].

For the second and inductive iteration, we used online documents of IS certifications from eight prominent and well-known certification authorities (e.g., *TrustedShops, McAfee SECURE Seal*) and two related international standards in the context of IS (e.g., *ISO/IEC 27001*). To identify new subsets of objects, we again applied content analysis. Due to the familiarity with the terminology, we only needed one iteration resulting in Krippendorff's $\propto$ of 0.93 [29]. We identified three new dimensions and added one characteristic to three existing dimensions, whereas we also renamed some characteristics.

For the third iteration, we analyzed current related research to IS certifications. With this, we used a deductive approach to conceptualize new characteristics and dimensions. Due to sparsity of research on IS certifications' characteristics, we only identified four relevant articles for our taxonomy development [1, 2, 8, 30]. By analyzing the articles in detail, we renamed seven characteristics and added four characteristics to existing dimensions.

For the fourth and inductive iteration, we conducted 19 one-to-one semi-structured interviews with organizations that already adopted IS certifications to identify new subsets of objects. Two researchers applied first selective coding to analyze interview transcripts to validate existing dimensions and characteristics, and second applied open coding to reveal additional relevant data and characteristics [14, 31]. With these coding techniques, we identified 23 codes related to 254 text segments, revealed two new dimensions, renamed two dimensions, and added in total four new characteristics to existing dimensions.

For the fifth and deductive iteration, we scheduled a workshop with three researchers to conceptualize new characteristics and dimensions. These researchers have a multi-year experience in IS certification research and developing novel IS certifications. In the workshop, we excluded six dimensions because, for example, the dimension was not relevant for organizations' evaluations, such as '*certification authorities have an example of the seal on their website*'. Moreover, we added one characteristic to existing dimensions, renamed in total seven dimensions, and identify six new dimensions (e.g., *surveillance frequency*).

For the sixth and inductive iteration, we conducted five semi-structured one-to-one interviews with consumers, having different experiences in using IS. We applied the same coding strategy as in the fourth iteration [14, 31]. Thereby, we identified 23 codes related to 80 text segments, leading to one new characteristic for an existing dimension.

For the seventh and deductive iteration, we again scheduled a workshop with four researchers to conceptualize new characteristics and dimensions. In this deductive iteration, we reconsidered and discussed the taxonomy and tried to identify missing dimensions and characteristics. We identified two new dimensions during the workshop, renamed dimensions, and added one characteristic to existing dimensions. We also excluded six dimensions that are only related to the certification authority and have no influence on evaluating a specific certification (e.g., *company size, product portfolio*).

For the eighth iteration, we used a new set of IS certifications and standards in an inductive approach. In particular, we applied the taxonomy to classify existing IS certifications to identify new subsets of objects. With this iteration, we not only were able to validate the applicability of our taxonomy, but we also did not identify any new objects, dimensions or characteristics. By repeatedly reviewing whether the five subjective and eight objective ending condition may be fulfilled, we concluded that all ending conditions are met.

4 A TAXONOMY ON IS CERTIFICATIONS

Our final taxonomy of key characteristics for IS certifications includes 17 dimensions, comprising a total of 46 characteristics (Table 2). We also grouped the dimensions into objective dimensions that can be characterized by observing measurable facts, and subjective dimensions that require personal opinions, assumptions, and beliefs from the organization, other stakeholders, or the general market to characterize an IS certification.

4.1 Objective Dimensions and Assigned Characteristics of IS Certifications

The **certification target** dimension explains what object an IS certification addresses. To determine the characteristics, we refer to the conformity assessment standards *ISO/IEC 17021 and 17065* that differentiate between four certification targets: (1) *management system*, the system managing the relevant aspects of its activities; (2) *product*, the result of a process (e.g., hardware or software); (3) *process*, the set of interrelated or interacting activities; and (4) *service*, the result of an activity necessarily performed at the interface between the organization and the consumer. Organizations need to select suitable IS certifications that match the object to be certified.

The **certification scope** is important because the scope also relates to certification efforts, costs, and complexity. While organizations might adopt a *narrow* certification (i.e., single quality like data protection) to internalize best practices, for example, regarding development and operation techniques enabling energy-efficient computing ('green IT'), other organizations may aim for *wide* certifications (i.e., multiple qualities like data protection, complaints management, and buying protection) to internalize various best practices and tackle consumer uncertainties regarding IS usage. Narrow certifications might be less costly and complex, and thus, easier to understand for organizations and its employees, whereas wide certifications can model highly interdependent system qualities, such as security and data protection.

Certifications are often split into different levels based on the scope or attestation method, such as a bronze, silver, and gold certification. The **assurance level** (i.e., *single* level or *multiple* levels) provides organizations with a certain flexibility, allowing them to select and adjust the certification efforts and better position themselves in the market.

Each certification is based on a criteria catalogue, specifying the requirements that a certification target has to fulfill. This criteria catalogue is typically based on *norms*, *regulations*, *best practices*, or *self-developed* (e.g., building on regulations and adding additional certification criteria). Organizations should consider the **criteria catalogue base** because it has several implications. For example, certifications building on norms (e.g., *ISO/IEC 27001*) and regulations (e.g., cloud service certification *AUDITOR* building on the GDPR) are more valuable due to their transparency and market perception. Self-developed criteria catalogues, may address novel problems that are not adequately covered by existing standards and best practices but might lead to lock-in effects, where an organization adjusts internal processes and their IS, and therefore gets dependent on the certification.

For the dimension **criteria catalogue accessibility**, we distinguish between *public access* (e.g., available on the certification authority's website), *on-demand accessible* (e.g., request via e-mail), or that the criteria catalogue is *not accessible before adoption* (e.g., proprietary IS certification). Accessibility is important because many organizations perform self-assessments to determine whether they can pass the certification before adopting a certification. In addition, consumers frequently inform themselves about the certification's content to make better decisions, when comparing IS.

The **geographic reach** dimension seeks to explain where an IS certification is acknowledged and recognized. It differentiates between one single country (*national*), a federation of states of one continent (such as the European Union; *international*), countries over several continents (*multinational*), and worldwide (*global*). Achieving a global reach is challenging for IS certifications because of national standards and regulations that dominate, and opposing opinions about the appropriateness and effectiveness of a certification. Having a higher geographic reach is a signal for high certification maturity but may also result in price premiums.

For the **pricing model***,* we distinguish between different pricing models that are applied to acquire IS certifications. The pricing can be a *fixed price*, *a graduated price model* based on, for example, the audit extent (e.g., Norton SECURED), or *a modular price model* (e.g., TrustedShops), for example, adjusted to the organization's turnover.

The **mandatory adoption** dimension differs between *mandatory* (e.g., *TISAX* for information security in the automotive industry) and *voluntary* (e.g., *TrustedShops* in electronic markets).

The **audit process** correlates with the credibility and effort of assessment results. Whereas a *self-assessment* by the organization requires less effort, a *third-party assessment* induces higher credibility of the certification, and the organization get expert feedback from an independent party that can then be internalized. In a *hybrid* audit process certification authorities rely on self-assessments and conduct assessments themselves.

Likewise, the **audit location** can be *on-site* (e.g., physical audit of the organization like a workshop or an inspection of the data center), *remote* (e.g., mainly digital audit via video calls [30]), or *hybrid* (e.g., combination of remote and on-site audits). Certifications performing on-site assessments are typically more credible due to richer insights than performing pure remote assessments.

The **surveillance frequency** refers to the frequency of audits to assess adherence to the criteria (e.g., ongoing compliance). An organization can be audited *continuously*, *within a year*, *after several years*, or even *only initially* and not afterward [30]. While most certifications require yearly surveillance, researchers and practitioners have started to develop continuous certification approaches that use automated monitoring and auditing techniques to prove ongoing compliance with certification criteria [20]. A shorter surveillance frequency indicates more constant monitoring of conformity with the certification criteria, and thus non-compliance with criteria can be revealed earlier [30]. However, more frequent audits also induce more costs and ongoing efforts.

For the **confirmation mechanism** dimension, organizations should evaluate whether the certification offers mechanisms to verify the authenticity of an issued certification (e.g., unique certification numbers, registers of issued certifications, or redirecting consumers to the certification authority website when they click on the IS certification seal). The confirmation mechanism can help organizations to signal trustworthiness and reliability of an issued IS certification while reducing the risk of fake images in the form of seals on organization's website (called '*fake seals*').

A certification authority issues each certification as an independent party. The **certification issuance license** dimension explains whether the license of an IS certification is *proprietary,* thus, the

Table 2: Taxonomy of key characteristics of IS certifications

Objective dimensions				
Certification target	Management system	Product	Process	Service
Certification scope	Narrow	Wide		
Assurance level	Single	Multiple		
Criteria catalogue base	Norm	Regulation	Best practice	Self-developed
Criteria catalogue Accessibility	Publicly accessible	On-demand accessible	Not accessible before adoption	
Geographic reach	National	International	Multinational	Global
Pricing model	Fixed	Graduated	Modular	
Mandatory for adoption	Mandatory	Voluntary		
Audit process	Third-party assessment	Self-assessment	Hybrid	
Audit location	On-site	Remote	Hybrid	
Surveillance frequency	Continuous	Intra-year	Multi-year	None
Certification authority accreditation	Mandatory	Voluntary		
Confirmation mechanism	Yes	No		
Certification issuance License	Proprietary	Generic		
Subjective dimensions				
Reputation	High	Low		
Diffusion	Wide	Sparse		
Appropriateness of meta-information	Appropriate	Inappropriate		

certification can only be issued by a single authority (i.e., possible negative consequences such as lock-in effects and monopolies); or *generally accessible,* therefore usable by several certification authorities (i.e., greater choice freedom, and emerging competitive dynamics).

The **certification authority accreditation** dimension explains whether a certification authority has to be accredited by an independent authority to issue the IS certification or not (e.g., mandatories of accreditation while issuing certifications proving GDPR compliance). Accreditation by responsible national accreditation bodies ensures the reliability, credibility, and comparability while signaling the certification authority's experience, knowledge, and technical capacity to perform its activities.

4.2 Subjective Dimensions and Assigned Characteristics of IS Certifications

The **reputation** dimension refers to the effectiveness and trustworthiness while seeking to explain whether an IS certification is well-established (*high reputation)* or less known and perhaps new (*low reputation*).

For the **diffusion** of an IS certification, the characteristics *wide* and *sparse* explain how often the IS certification is used in practice by other organizations. A high diffusion may reflect the degree of maturity of the certification whereas in some cases that might lead to negative effects (e.g., less worth when everyone can achieve it). However, a new IS certification can also be an opportunity to differentiate an organization from competitors, achieving competitive advantages.

For the **appropriateness of meta-information**, we refer to an organization's evaluation of the additional information (e.g., date of expiration, consumer feedback, or the criteria catalogue base) that can be presented with an IS certification and can vary from *appropriate* to *inappropriate.* A lack of meta-information might lead to consumer confusion (e.g., clearness of the target of certification–a common issue with *ISO/IEC 27001* certifications), however consumer reviews might be perceived as inappropriate (i.e., mingling of second- and third-party information and bears the risk of negative consumer reviews).

5 DISCUSSION

5.1 Principal Findings

The growing importance and diversity of IS certifications in electronic markets challenge the selection of appropriate certifications for organizations that need to satisfy manifold internal and external forces. This study provides a taxonomy of IS certification's key characteristics to extend our understanding of what is important when evaluating certifications. Synthesizing the results from a taxonomy perspective not only provides a unique opportunity to research the influence of multiple IS certifications simultaneously but enables us to understand the differences and unique attributes of IS certifications.

Before evaluating IS certifications, organizations should decide whether to use an IS certification for mainly internal reasons (e.g., for efficiency improvements, or cost savings), or external purposes, like increasing consumers' trust. Depending on this, the relevance of the individual dimensions may vary, possibly resulting in a change of evaluation results. For example, the dimension '*certification reputation'* might lose its importance when evaluating an IS certification for organizational improvements because the dimension depends on consumers' perceptions of the certification that impacts its effectiveness.

Even though most of the dimensions are underlying an objective decision, organizations must have a profound knowledge of the IS certifications in question to enable evaluation. Consequently, organizations must have access to all information that is required when evaluating IS certifications. However, classifying existing IS certifications following our taxonomy has revealed that certification authorities do not always provide the necessary descriptions and that gaining access to the information can be complex and challenging (i.e., accessing the criteria catalogue). This issue is even more crucial for the three subjective dimensions because they require knowledge on the certification market (i.e., relating to dimensions *reputation* and *diffusion*) and organization's internal and external needs and preferences (i.e., relating to the dimension *meta-information appropriateness*). Still, organizations can rely on available certification meta-frameworks (e.g., ENISA's meta-framework comparing cloud certifications) and (non-profit) communities that have formed over time, which, for example, elaborate on certifications' credibility and reputation (e.g., *Initiative D21* in Germany for webshops).

While we aimed to develop a taxonomy for IS certification's key characteristics, the high interdependence of IS certifications and certification authorities became apparent throughout our study. Typically, organizations evaluate IS certifications, select a set of candidates and then evaluate and compare available certification authorities before adopting a certification and setting up certification agreements with an authority. We initially incorporated more dimensions relating to the certification authority into the taxonomy (i.e., authority company size, location, structure, reputation, complaint management, and product portfolio). Yet, discussions in the seventh iteration revealed that these dimensions do not fit our meta-characteristic, instead, belonging to a taxonomy to classify certification authorities. We remained the dimensions *'certification authority accreditation'* and *'certification issuance license'* in our taxonomy due to their impact as the foundation for searching and evaluating certification authorities.

5.2 Theoretical and Practical Contributions

Our study has implications for research and practice. We advance research by developing a taxonomy as a means to cut through the jungle of multiple IS certifications, which was mostly overlooked in research. Researchers mostly considered a single certification where they mainly focused on the adoption process [e.g., 11, 12, 13]. With our consideration of multiple IS certification, we contribute to research by supporting the evaluation process, and the perspective of multiple IS certifications, which were both mostly neglected so far in research.

While research has frequently analyzed whether or not the adoption of a certification will lead to internal benefits [e.g., 13, 23, 24] or change consumers' perceived assurance and trust perceptions [e.g., 7, 15], prior research only analyzes the impact of certifications from a black box perspective (i.e., adopted vs. not adopted a certification), and lacks a deep understanding about characteristics of certifications [1, 3]. Recent research started to identify structural blocks of IS certifications (e.g., content, source, and process) and highlights that these blocks impact consumers' certification perceptions [1]. Using taxonomy development as a research method, we identify the key characteristics of IS certifications and thus break down the structural blocks and provide more details on which characteristics of IS certifications are important and relevant for organizations. With this more fine-grained perspective, we provide key characteristics for an external purpose (e.g., building consumers' trust and signaling compliance with regulations) and for internal improvements of management processes (e.g., meeting privacy and security requirements). Thus, this taxonomy supports opening the prevalent black-box perspective in prior research by highlighting key characteristics that might be included in future research when analyzing certification adoption and effectiveness.

Besides theoretical implications, this work also has implications for practice. First, we provide organizations a classification of dimensions and key characteristics that enables the comparison of several IS certifications and the selection of the most suitable ones for organizations' specific use context. The taxonomy provides organizations which often struggle in evaluating IS certifications with a structure [1, 2]. This structure may help organizations to clarify the evaluation of the several possible IS certifications (e.g., *TrustedShops, McAfee SECURE Seal*) in a certain electronic market. Second, we provide the groundwork to improve the adoption of IS certifications. Since the evaluation is a preliminary process to the adoption process, we help organizations to ensure a successful and valuable application of IS certifications.

5.3 Limitations and Future Work

This study is subject to limitations. First, we struggled in building dimensions where the characteristics should explicitly cover all possible forms of objects of interest. For example, in the dimension '*certification scope'*, we could not explicitly list all the different qualities that can be certified as characteristics, such as data protection, IS security, or environmental sustainability. It is rather difficult to find consistent and unique characteristics for this dimension because IS certifications may provide individual assurances and bundle different assurances [8]. We, therefore, decided to include the characteristics *'wide'* and *'narrow'* instead. Second, our sample of objects is limited to IS certifications that are applied in practice. Without question, there are more certifications in an IS use context or are currently developed (e.g., *AUDITOR* for cloud services). However, due to the number of different iterations, such as our survey or our in-depth expert interviews, we are confident that our taxonomy represents a good starting point to classify the key characteristics when evaluating IS certifications. Adding to this, our taxonomy fulfills all ending conditions defined by Nickerson et al. [14] and can, therefore, be extended or adjusted where necessary. Third, we introduced subjective and objective dimensions. Although the taxonomy helps understand the evaluation of IS certifications, organizations still need to have profound knowledge on IS certifications when classifying objects, especially for subjective dimensions.

Our taxonomy can be treated as a starting point for further investigations. First, we call upon future research to investigate the interdependencies between our taxonomy dimensions to increase the understanding of evaluating IS certifications. Due to the research method's consistency and robustness [14], we avoid this investigation in taxonomy development. Nevertheless, it can be interesting to compare how these dimensions relate to each other and which ones are possibly more important for organizations and which are less important. Second, the role of the certification authority was mentioned but not further investigated. Especially, we encourage scholars to examine the key characteristics of certification authorities to ease the evaluation process.

6 CONCLUSION

IS certifications are considered as a powerful tool to improve the security and trustworthiness of an IS. Notwithstanding the positive impact of consumers' prevailing uncertainty or the achievement of internal management practice improvements, organizations struggle to evaluate and finally adopt appropriate IS certifications. With our research, we help organizations compare several IS certifications and finally select the most suitable one for the specific use context of organizations. To this end, our main contribution is a taxonomy of IS certifications concerning key characteristics that might impact the evaluation process. Our taxonomy consists of 17 dimensions, comprising 46 characteristics. It highlights that not only objective but also subjective characteristics can impact the evaluation of IS certifications. Based on our taxonomy, further research should investigate the interdependencies between our taxonomy dimensions to increase the understanding of evaluating IS certifications.

ACKNOWLEDGMENTS

Financial support for this work by the German Research Foundation (DFG) through the granted research project "A Decompositional Analysis of IT Certifications in Electronic Markets and their Effect on Platform Customer and Provider Perceptions" (BE 4308/4-1 and SU-717/10-1) is gratefully acknowledged.

REFERENCES

[1] Lansing, J., Benlian, A. and Sunyaev, A. 2018. "Unblackboxing" Decision Makers' Interpretations of IS Certifications in the Context of Cloud Service Certifications. Journal of the Association for Information Systems, 19, 11 (December 2018), 1064-1096. https://doi.org/10.17705/1jais.00520

[2] Lins, S. and Sunyaev, A. 2017. Unblackboxing IT Certifications: A Theoretical Model Explaining IT Certification Effectiveness. In Proceedings of the International Conference on Information Systems (ICIS'17). Seoul.

[3] Löbbers, J., Lins, S., Kromat, T., Benlian, A. and Sunyaev, A. 2020. A Multi-Perspective Lens on Web Assurance Seals: Contrasting Vendors' Intended and Consumers' Perceived Effects. Electronic Commerce Research (May 2020). https://doi.org/10.1007/s10660-020-09415-2

[4] ISO The ISO Survey. International Organization of Standardization, 2018.

[5] Gao, L. and Waechter, K. A. 2017. Examining the role of initial trust in user adoption of mobile payment services: an empirical investigation. Information Systems Frontiers, 19 (June 2017), 525-548. https://doi.org/10.1007/s10796-015-9611-0

[6] Lee, M. and Lee, J. 2012. The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. Information Systems Frontiers, 14, 2 (April 2012), 375-393. https://doi.org/10.1007/s10796-010-9253-1

[7] Özpolat, K., Gao, G., Jank, W. and Viswanathan, S. 2013. The Value of Third-Party Assurance Seals in Online Retailing: An Empirical Investigation. Information Systems Research, 24, 4 (July 2013), 1100-1111. https://doi.org/10.1287/isre.2013.0489

[8] Lansing, J., Siegfried, N., Sunyaev, A. and Benlian, A. 2019. Strategic signaling through cloud service certifications: Comparing the relative importance of certifications' assurances to companies and consumers. The Journal of Strategic Information Systems, 28, 4 (December 2019). https://doi.org/10.1016/j.jsis.2019.101579

[9] Kim, K. and Kim, J. 2011. Third-party Privacy Certification as an Online Advertising Strategy: An Investigation of the Factors Affecting the Relationship between Third-party Certification and Initial Trust. Journal of Interactive Marketing, 25, 3 (2011), 145-158. https://doi.org/10.1016/j.intmar.2010.09.003

[10] Gopal, A. and Gao, G. 2009. Certification in the Indian Offshore IT Services Industry. Manufacturing & Service Operations Management, 11, 3 (June 2009), 471-492. https://doi.org/10.1287/msom.1080.0234

[11] Djofack, S. and Camacho, M. A. R. 2017. Implementation of ISO 9001 in the Spanish tourism industry. International Journal of Quality & Reliability Management 34, 1 (January 2017), 18-37. https://doi.org/10.1108/IJQRM-10-2014-0151

[12] Heras-Saizarbitoria, I. and Boiral, O. 2013. ISO 9001 and ISO 14001: Towards a Research Agenda on Management System Standards. International Journal of Management Reviews, 15, 1 (September 2013), 47-65. https://doi.org/10.1111/j.1468-2370.2012.00334.x

[13] Nair, A. and Prajogo, D. 2009. Internalization of ISO 9000 Standards: The Antecedent Role of Functionalist and Institutionalist Drivers and Performance Implications. International Journal of Production Research, 47 (August 2009), 4545-4568. https://10.1080/00207540701871069

[14] Nickerson, R. C., Varshney, U. and Muntermann, J. 2013. A method for taxonomy development and its application in information systems. European Journal of Information Systems, 22, 3 (December 2013), 336-359. https://doi.org/10.1057/ejis.2012.26

[15] McKnight, D. H., Kacmar, C. J. and Choudhury, V. 2004. Shifting Factors and the Ineffectiveness of Third Party Assurance Seals: A Two-Stage Model of Initial Trust in a Web Business. Electronic Markets, 14, 3 (September 2004), 252-266. https://doi.org/10.1080/1019678042000245263

[16] Adam, M., Niehage, L., Lins, S., Benlian, A. and Sunyaev, A. 2020. Stumbling over the trust tipping point – The effectiveness of web seals at different levels of website trustworthiness. In Proceedings of ECIS 2020 Marakesh

[17] Lins, S., Kromat, T., Löbbers, J., Benlian, A. and Sunyaev, A. 2020. Why Don't You Join In? A Typology of Information System Certification Adopters. Decision Sciences, forthcoming (September 2020). https://doi.org/10.1111/deci.12488

[18] Lynn, T., van der Werff, L., Hunt, G. and Healy, P. 2016. Development of a Cloud Trust Label: A Delphi Approach. Journal of Computer Information Systems, 56 (July 2016), 185-193. https://doi.org/10.1080/08874417.2016.1153887

[19] Lins, S., Schneider, S. and Sunyaev, A. 2018. Trust is Good, Control is Better: Creating Secure Clouds by Continuous Auditing. IEEE Transactions on Cloud Computing, 6 (January 2018), 1-14. https://doi.org/10.1109/TCC.2016.2522411

[20] Lins, S., Schneider, S., Szefer, J., Ibraheem, S. and Ali, A. 2019. Designing Monitoring Systems for Continuous Certification of Cloud Services: Deriving Meta-requirements and Design Guidelines. Communications of the Association for Information Systems (April 2019), 406-510. https://doi.org/10.17705/1cais.04425

[21] Löbbers, J. and Benlian, A. 2019. The effectiveness of IS certification in E-commerce: does personality matter? Journal of Decision Systems, 28 (May 2019), 1-27. https://doi.org/10.1080/12460125.2019.1684867

[22] Naveh, E. and Marcus, A. 2004. When Does the ISO 9000 Quality Assurance Standard Lead to Performance Improvement? Assimilation and Going Beyond. Engineering Management, IEEE Transactions on, 51 (August 2004), 352-363. https://doi.org/10.1109/TEM.2004.830864

[23] Martínez-Costa, M., Martínez-Lorente, A. R. and Choi, T. Y. 2008. Simultaneous consideration of TQM and ISO 9000 on performance and motivation: An empirical study of Spanish companies. International Journal of Production Economics, 113, 1 (May 2008), 23-39. https://doi.org/10.1016/j.ijpe.2007.02.046

[24] Prajogo, D., Tang, A. K. Y. and Lai, K.-h. 2012. Do firms get what they want from ISO 14001 adoption?: an Australian perspective. Journal of Cleaner Production, 33 (September 2012), 117-126. https://doi.org/10.1016/j.jclepro.2012.04.019

[25] Ismyrlis, V. and Moschidis, O. 2015. The effects of ISO 9001 certification on the performance of Greek companies. The TQM Journal, 27, 1 (January 2015), 150-162. https://doi.org/10.1108/TQM-07-2013-0091

[26] Arauz, R. and Suzuki, H. 2004. ISO 9000 performance in japanese industries. Total Quality Management & Business Excellence, 15, 1 (January 2004), 3-33. https://doi.org/10.1080/1478336032000149072

[27] Tarí, J., Molina-Azorin, J. and Heras-Saizarbitoria, I. 2012. Benefits of the ISO 9001 and ISO 14001 standards: A literature review. Journal of Industrial Engineering and Management, 5 (December 2012), 297-322. https://doi.org/10.3926/jiem.488

[28] Pheng, L. and Tan, J. 2005. Integrating ISO 9001 Quality Management System and ISO 14001 Environmental Management System for Contractors. Journal of Construction Engineering and Management, 131 (Novembre 2005). https://doi.org/10.1061/(ASCE)0733-9364(2005)131:11(1241)

[29] Krippendorff, K. 2004. Content Analysis: An Introduction to its Methodology. Thousand Oaks, CA: Sage. (2004).

[30] Schneider, S., Lansing, J., Fangjian, G. and Sunyaev, A. 2014. A Taxonomic Perspective on Certification Schemes: Development of a Taxonomy for Cloud Service Certification Criteria. In Proceedings of 47th Hawaii International Conference on System Sciences (HICSS'14). 4998-5007. https://doi.org/10.1109/hicss.2014.614

[31] Myers, M. D. 2013. Qualitative Research in Business & Management. Sage Publ, London (2013).