applied sciences

MDPI

Article

Governance, Risk, and Compliance in Cloud Scenarios

Knud Brandis [1], Srdan Dzombeta [1], Ricardo Colomo-Palacios [2,*] and Vladimir Stantchev [3]

[1] PwC Cybersecurity Services GmbH, Kapelle-Ufer 4, 10117 Berlin, Germany; kbrandis@pwc-cybersecurity.com (K.B.); sdzombeta@pwc-cybersecurity.com (S.D.)
[2] Department of Computer Sciences, Østfold University College, B R A Veien 4, 1783 Halden, Norway
[3] Institute of Information Systems, SRH Hochschule-Berlin, Ernst-Reuter-Platz 10, 10587 Berlin, Germany; vladimir.stantchev@srh-hochschule-berlin.de
* Correspondence: ricardo.colomo-palacios@hiof.no; Tel.: +47-6921-5000

Received: 21 December 2018; Accepted: 13 January 2019; Published: 17 January 2019

Featured Application: The current article proposes a framework to guide compliance efforts in organizations with cloud computing infrastructures.

Abstract: Cloud computing is changing the way organizations approach technology and its infrastructure. However, in spite of its attractiveness, cloud computing can be seen as a threat in terms of compliance. Given its intrinsic distributed nature, regulations and laws may differ and customers and cloud providers must find a way to balance increasing compliance pressures with cloud computing benefits. In this paper, the authors present a framework aimed to help organizations to cope with compliance aspects in their cloud-oriented environments. Built upon current literature on the topic and qualitative approaches, the framework has been implemented in two organizations. Results from its contribution are encouraging, leading to adopter organizations to less reported compliance violations and higher contribution of cloud computing to overall quality of service and organizational compliance management.

Keywords: IT governance; cloud computing; risk; compliance; enterprise architecture management

1. Introduction

Given the increasing importance of IT in society, its governance has been attracting attention in the last years from academics and practitioners alike. Now, IT governance is seen as a key topic for organizations and interest is rooted in the changing role and relevance of IT within organizations [1]. There are many definitions for IT governance published in the scientific literature. A good review on the definitions and orientations on IT governance can be found in recent works [2,3]. Generally, IT governance is about the configuration of organizational resources to ensure effective management of IT. However, there are more specific definitions on the term. Weill and Ross define IT governance as "specifying the decision rights and accountability framework to encourage desirable behavior in using IT" [4]. IT governance as a field of study is based on several previous research fields, including, and according to [5], corporate governance models, corporate strategies, IT knowledge of business divisions, and power of an IT organization.

One of the aspects that is crucial for IT governance is the correct alignment of IT and corporate strategy. In IT and business alignment, the works of Luftman, with his Strategic Alignment Maturity Model (SAMM), are the most relevant publications on the topic [6], after the pioneering work by [7].

Benefits of IT governance have been reported largely in the literature. Perhaps the most important finding of all is the one backed up by Van Grembergen and De Haes [8], indicating that IT governance enables IT-business alignment, which then contributes to firm performance. This finding is also reported by other authors on studies devoted to IT governance, but focused on the Chief Information

Officer (CIO) role, e.g., [9,10], examining financial performance [1] or relational performance [11], citing just some of the most recent and relevant cases. Perhaps because of this, IT governance is seen as a key aim of the information management function and also as imperative for organizations to meet their business activity [12].

Given the crucial importance of the topic, researchers devoted their time to build frameworks and initiatives devoted to IT governance. For instance, "COBIT: Control Objectives for Information and Related Technologies" was launched by the American "Information System Audit and Control Association" [13]. COBIT is a well-known IT governance framework to implement a set of best practices for management, control, and assurance of IT [14]. COBIT 4.1 describes 34 high-level control objectives and 210 detailed control objectives. Other initiatives worth mentioning is the one led by "MIT: Massachusetts Institute of Technology" [15] and also the one conducted in the Software Engineering Institute: Capability Model Integration for Services (CMMI-SVC) [16].

The set of previous initiatives led to the definition of a standard for IT governance. Consequently, the ISO38500:2008 was produced in May 2008. This standard was highly influenced by the Australian Standard for Corporate Governance of Information and Communication Technology AS8015-2005 published in January 2005. ISO38500:2008 stands for a framework, including three different tasks for IT governance, namely: (1) Assessment of the use of IT; (2) preparation and implementation of plans and policies; and (3) the monitoring of conformance to policies and performance against the plans.

As a consequence of the importance of the topic, the literature reports a set of studies on the application of IT governance to different functional scenarios, including education [17–19], financial organizations [20–22], public sector [23–26], life sciences [27,28], or Small and medium-sized enterprises (SMEs) [29,30], naming just some of the most important studies.

Cloud computing has changed the IT scenario profoundly. Cloud is a technology that grew from distributed, grid, and utility computing [31], and is now one of the fastest growing segments of the IT industry. Not in vain, the worldwide public cloud services market is projected to grow by 17.33% in 2019 to a total of $206.2B, up from $175.8B in 2018 according to Gartner [32]. In this scenario, there are also threats. Thus, security, trust, and privacy remain challenges for organizations that adopt cloud computing [33,34] and the new privacy-related laws and regulations (Sarbanes-Oxley Act and general data protection regulation in Europe) will be an aspect to consider among its adopters [35].

Beyond regulations, there is a problem of compliance in cloud scenarios. Compliance can be defined according to the Merriam-Webster dictionary as:

(a) The act or process of complying to a desire, demand, proposal, or regimen or to coercion and;
(b) conformity in fulfilling official requirements.

A more specific definition can be found in the scientific literature: IT compliance is the accordance of corporate IT systems with predefined policies, procedures, standards, guidelines, specifications, or legislation [36]. Cloud technology is distributed in an intrinsic way and as a consequence of this, compliance is a shared responsibility among organizations and service providers; it involves service providers, service brokers, customers, and auditors [37]. According to [38], the intrinsic nature of the cloud leads to almost all kinds of compliance challenges.

Compliance requirements can be rooted in internal and external regulations. With regards to internal regulations, they comprise guidelines or operating procedures. On the other hand, external regulations are laws, regulations, or civil contracts. This complex scenario becomes even more convoluted and industry-specific requirements may arise in industries, like banking, health, insurance, or the public sector. There is a need to identify the set of compliance requirements to ensure a feasible risk management. However, in cloud settings these requirements are blurred in many cases. This complexity depends on the data type and the cloud service structure and service. The complexity of compliance in the cloud is rooted in the sheer number and complexity of laws and regulations that need to be observed in cloud settings [39]. In this scenario, there are opportunities and barriers towards service adoption and the market for cloud operators and tenant communities alike.

Literature underlined the need to perform research on ways to help IT companies in the management of possible overlapping or conflicting regulatory compliance requirements [40]. Moreover, the literature has recommended more research on the topic to overcome compliance challenges in cloud settings [37,41]. Answering this call for research on the topic, the main contribution of the paper is a framework to help organizations in the adoption and management of cloud scenarios based on a proper classification of risks taken by such organizations with regards to compliance aspects. These risks are classified as cultural, legal, technical, and organizational. The authors define a process to manage these risks following previous sound approaches in the area of risk management in cloud settings [41]. This contribution is presented from the viewpoint of the design of the framework in Section 2. In order to validate the framework, which is the main contribution of the work performed, Section 3 introduces the two case studies conducted, presenting their internals and main results. Section 4 depicts the main limitations of this work, summarizes the paper, and proposes future work.

2. The Framework

In this section, the framework, defined to integrate aspects of compliance in cloud computing environments, is introduced. To do so, in the next subsections, firstly, the motivation and the overall picture as well as the main components of the framework are introduced. In the second term, the validation conducted by experts is presented.

2.1. Rationale and Summary

The framework is aimed to provide compliance in cloud computing scenarios. This is realized by first soliciting relevant input from its five main aspects, namely: Legal, organizational and processual, technological, and, finally, cultural. For each of these aspects, a specific questionnaire was designed. These questionnaires served to automate requirements' collection and categorization based on a set of fixed questions. Results gathered in as inputs were then processed in the so called inner works of the framework. This is a compliance management (CM) approach for handling cloud computing change requests that include new services or methods. In sum, the framework contains a set of questionnaires to classify inputs and an inner part that is able to transform these inputs into a potential risks evaluation.

The overview of the framework is shown in Figure 1.

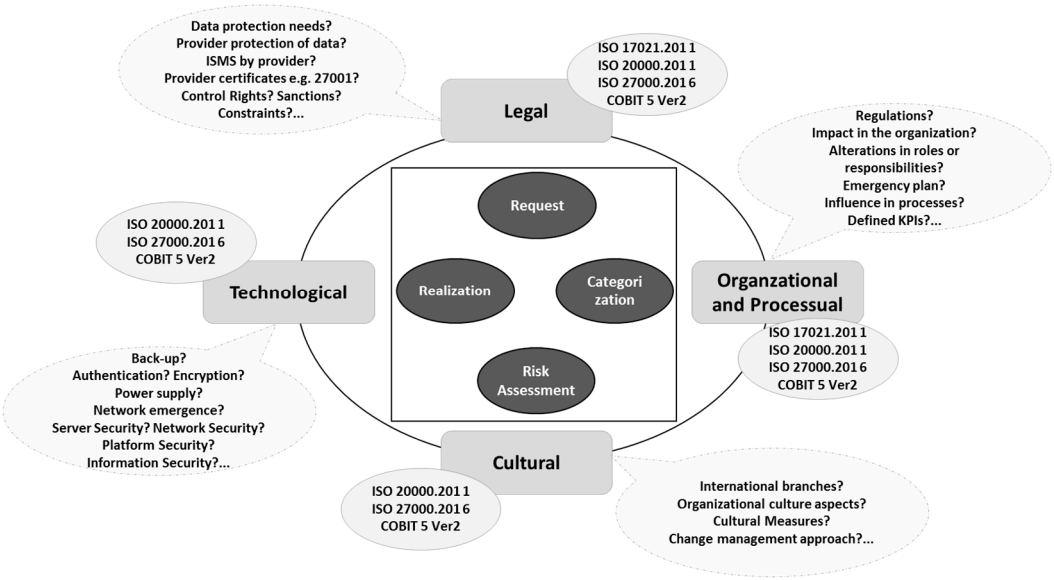

Figure 1. Overview of the main aspects of the developed framework, including the influences of standards to each aspect and features to consider.

In the next section, the different aspects in the framework are depicted.

2.1.1. Legal

There is a need to customize the framework in a functional scenario and country, given that laws are different in different areas of application. In this case, the authors customized the legal aspect for the healthcare sector providers in Germany. The internals of these aspects were presented by authors [28]. The specific questionnaire defined included this set of questions (all questions are presented in their final form):

1. What types of data are influenced by the subcontracting approach? Significant data, such as health, social, or private clinical data?
2. What types of legitimate outlines can be used?
3. What are the possibilities if subcontracting takes place: Either of data being available, confidential, or integrable?
4. What are the necessities to protect the data? Deciding on suitable security architecture, encryption and cryptography of data, authorization management, managing potential risks, management of the occurrences of security issues, measuring and planning of contingency, and other concerns regarding the data protection.
5. Whether the legal and data protection necessities are met by the provider?
6. Whether the supplier has the required information security management system (ISMS)?
7. Measuring the extent to which the ISMS is assessed with respect to the suitability of the technical and organizational level and how are the outcomes are documented?
8. Whether the supplier has the required up-to-date and international certificates (for example, ISO 27001)?
9. Whether the cloud computing service is formulated neatly and obviously or not?
10. Whether the control rights of the organization using the cloud along with the required obligations for the supplier of the cloud service are specified or not?
11. Are there some rules supporting the probable operations and the retrieval of data if the cloud service provider commits any bankruptcy?
12. Whether any explicit and appropriate service-level agreement are available? If yes, whether they ensure the requirement of availability and dependability, deadlines for restoration and response, computing power, and support specifics?
13. In case of disastrous failures, are there any particular business community management (BCM) guidelines?
14. Whether controls are carried out regularly? Additionally, whether there exists any evaluations of the agreed upon technical and organizational measures?
15. Whether the security aspects are being assessed regularly and whether they are up-to-date and belong to the recent state of the art?
16. Whether the international data communication is influenced by the adjustments?
17. Whether sanctions are foretasted?
18. Whether any access points exist for state agencies (e.g., National Security Agency, NSA)?
19. Whether there exist any specific constraints?

2.1.2. Organizational and Processual

In this case, taking into account that the cloud is based on service oriented architecture (SOA), the questionnaire is designed combining SOA governance models and SAM [6]. The questionnaire presents this set of questions that includes in this case a set of sub questions:

1. Are there regulations for the introduction of the alteration in processes and in their steps?

- What effects do the alterations have over other processes?
- What effects do these alterations have over the corporate strategy?
- Whether the consideration of security concepts is assured when the alterations are taking place?
- Whether the changes are well planned, evaluated, accepted, and documented?
- Whether the alternative solutions are produced before the development of the changes?
- Whether the information security management is taken into consideration in all the alterations?

2. Whether the significant organizational processes are impacted?

- What is the level of data availability?
- What is its influence on other activities?

3. Whether there are any alterations in responsibilities and roles due to the changes?
4. Plan for emergency.

- Evaluation of the most recent emergency tests documents.
- Security aspects.
- Regular security valuations at the Content Security Policy (CSP) and other suppliers by a qualified third party.
- Authentication, authorization, administration, inspections, and attentiveness access control.
- Processing the data is only permitted based on the guidelines of the cloud user and the usage of data by the CSP for their own purposes is not allowed.
- Test of influence of the CSP and other providers.
- The cloud user should be able to monitor and they should be able to prove the service level agreement (SLA) fulfilment.
- The administrative processes should be monitored and logged.
- Four-eyes-principle at the time of significant administration processes.
- CSP preparation of log files.
- Information about security events.
- Round the clock response group available for security event management and troubleshooting.
- Round the clock handling of cloud services and a rapid response to security events.
- Employment of appropriate measures in contradiction of domestic intimidations that are characteristic of a multi-tenant architecture.
- Formation of transparency and trust by the establishment of thorough information anticipated for the cloud user.
- Measures at the employees' level.
- Police certificate/clean criminal record.
- Educational history, qualifications, and present and previous affiliations.
- Personal setting (e.g., party membership).
- IT security courses.
- Social engineering courses.
- Control and education for the purpose of understanding.
- Assessment of workers (e.g., technicians, facility managers).
- Agreement for data security and non-disclosure.

5. What are the processes influenced?

- Corresponding to their fields, e.g., "governance activities"," customer-facing activities", "core activities", and "support activities";

- Corresponding to their inevitability and significance, e.g., "must do", "nice-to-have", "delighter".

6. Are business affected analyses carried out?
7. Are there explicit described approaches and connected key performance indicator (KPI)s for them at the procedure level?

2.1.3. Technological

The questions present in the questionnaire are based on two different models: Wheeler's e-business innovation cycle [42] and the technology acceptance model (TAM) [43]. TAM is based on the theory of reasoned action (TRA). The TRA theorizes that the intention to accept or reject a particular technology is based on a series of trade-offs among the perceived benefits of the technology to the user and the effort of learning or using the given system. According to this model, two major factors determine behavioral intentions, namely: User attitude toward the behavior and subjective norms. Figure 2 below shows how TAM suggests users come to accept and use technology through the evaluation of different factors, such as perceived usefulness (degree to which a person believes that using a particular system would enhance his or her job performance) and perceived ease-of-use (the degree to which an individual believes that using a particular system would be easy).

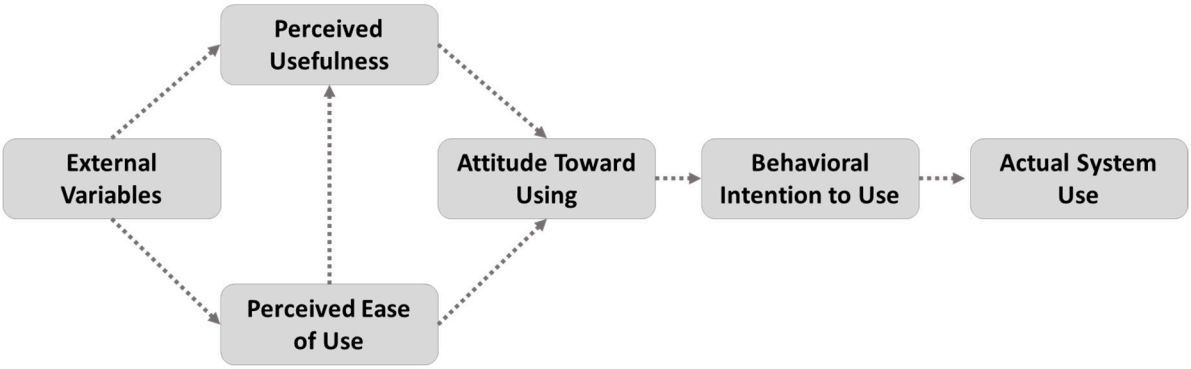

Figure 2. Technology acceptance model (TAM) dimensions.

The questionnaire is as follows:
1. What are the technologies accessible for user and access management, role-based access control, two factor authentication?
2. What are the feasible technologies for encryption at the time of data processing and data transportation?
3. What are the feasible technologies for data backup, repair, and accessibility of the service?
4. What are the technologies accessible for the supply of power, heating, ventilation, and air conditioning (HVAC), and water?
5. What are the technologies accessible for fire protection?
6. What are the technologies accessible for vigorous structure, unnecessary network connection, emergency working places, etc.?
7. What are the technologies accessible for unnecessary data centers, documentation, and control of obtainability management?
8. What are the technologies accessible for facility security, access control, and secure entrance area?
9. What are the technologies accessible for control of service suppliers (cleaning, facility management, repair technicians)?
10. What are the technologies accessible for promising server security?

- Host protection (firewall, intrusion detection, integrity examination).
- Secure standard configuration (strengthen operating system).

- Sandboxed environment for each virtual machine.
- Certified hypervisors (at least CC EAL4, IT SEC E3), avoiding hyperjacking and including embedded hypervisors.
- Superfluous images/services of the provider.
- A protected sandbox environment in the case of Infrastructure as a Service (IaaS) to avoid the harnessing of host systems.
- Systems ready for valuation of system documentation, status, and log files.

11. What are the technologies accessible for network security?

- Superfluous network links.
- Protections against attacks, malware, and viruses.
- Safe configuration of all cloud components, network division.
- Encrypted remote supervision.
- Encrypted communication between Content Security Policy (CSP) and the cloud user.
- Encrypted communication between various Cloud Computing (CC) sites.
- Encrypted communication to and from third-party servicers.
- Encrypted transmission of network management information.
- Evaluation of virtual private network (VPN) infrastructure and end-to-end encryption (E2EE) chain (including man-in-the-middle attacks and backdoors).

12. What are the feasible technologies for ensuring application and platform security?

- Incorporation of security in various activities namely, software life cycle, security gateways, vulnerability evaluation, code reviews, and audits.
- The isolation of application and monitoring of the interface.
- Automatically monitoring and assessing the user applications.
- Management of the patch and change and the compatibility test of patch.
- Checking if the secure application development is carried out according to the guidelines or not.

13. What are the feasible technologies to ensure information security?

- Management of patch and change.
- Customer data life cycle definition.
- Isolating securely.
- Information access based on role, for example, based on Lightweight Directory Access Protocol (LDAP).
- Routine backups (extent, intervals, storage concept, times, and durations).
- Secure and complete removal.
- Every element of the system can be aimed at by an attack; hence, weaknesses and protection analysis.
- Measures are required (end-to-end security).

14. What are the accessible technologies aimed at ensuring encryption and key administration?

- Methods to be used are supposed to be assured and encrypted securely.
- Keys should be randomly generated with enough key length.
- The exchange of keys should be secure and asynchronous.
- The length of the keys should be short and their storage should be secure.
- Destruction of keys, for example, using Security Assertion Markup Language (SAML).
- Rigor verification of users in the cloud (two-factor authentication).

15. What are the accessible technologies to overcome the absence of standardization in CC?

- The customer should make sure the service supplier utilizes standardized technology and interfaces; this should be stated in its early stage of contract.
- Mix cloud methods to prevent compatibility issues between the cloud and IT systems in the customer's organization.

2.1.4. Cultural

The questionnaire is built in two different sources. Firstly, the Cultural Orientations Framework [44] and the cultural dimensions defined by Hofstede [45] are adapted to cloud service assessment. The set of questions is as follows:

1. What are the countries in which the main offices and branches of the organization are based?
2. What are the countries that the main accounts of the organization are included?
3. To what extent does the organization reach to the markets (regional, national, international, and world-wide)?
4. What are the existing cultural aspects to consider (e.g., a religious or non-profit organization, military, or other certain organizational surroundings)?
5. What are the related cultural aspects (based on Hofstede and following works) for the organization?
6. What are the measures for the related cultural aspects that may be required?
7. How are the required measures of the related cultural aspect accumulated?
8. What is the relevancy of every related cultural aspect for change management?
9. How are the related measures supposed to be considered while the change is carried out?
10. What are the related national cultural aspects to consider?
11. What are the most relevant organizational culture aspects?

2.1.5. The Inner Works

This aspect of the framework is designed to control changes on the overall architecture of adopters. This is the reason why a change management perspective is adopted. In order to do so, the authors adopted the approach proposed by Information Technology Infrastructure Library (ITIL) [46]. This approach ensures that changes are registered, scheduled, and managed in an efficient way and with controlled risk. The main steps in the ITIL change process are illustrated in Figure 3:

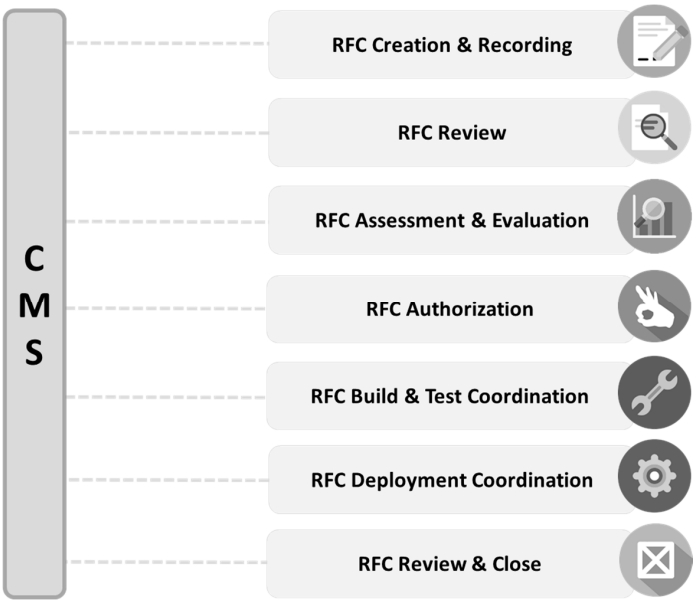

Figure 3. Change management process adapted from Information Technology Infrastructure Library (ITIL).

From the generic process defined by ITIL [46], the authors added the following steps in the review, assessment, and evaluation.

To do so, the following steps are defined:

1. Identifying the significant information and procedures as main assets of the organization.
2. Identifying the secondary assets for the association along with metrics (inheritance).
3. Description of security requirements for reflected information in cloud computing as well as the definition of total risk according to the potential harm and possibility.
4. Present status: Measures that already existed.
5. Assessment of risk of current measures and of reflected alteration (total risk).
6. Steps remaining and new measures or controls.

Once the process is defined, the next step is to define the protection requirements categories. The aim of these requirements is to decide for the affected data which protection requirements of the data presents in terms of availability, confidentiality, and integrity. Protection requirements are not easily quantifiable. Therefore, we divided the protection requirements into three qualitative categories as follows:

- Low. The effect of possible damage or harm is partial and foreseeable.
- Medium. The effect of possible damage or harm may be substantial.
- High. The effect of possible damage or harm may be of disastrous extents, which could intimidate the very existence of the organization.

The next step is the definition of damage areas to consider in each protection requirement:

- Legal: Disruptions of rules, guidelines, or agreements. Damage of the right to informational self-determination.
- Organizational/processual: Damaged ability to carry out the ongoing tasks, damage of business processes or activities, physical harm.
- Technical: Removal of a certain technology from the accepted assets list due to compromised security.
- Cultural: Negative external or internal impacts, cultural confusions.
- Financial penalties.

These categories (apart from the "financial" that can be considered as generic) correspond to the categories defined as subject field areas of the proposed framework. Table 1 presents a decision support tool to clarify the different damage areas combined with the different categories.

Table 1. Damage areas and categories: Examples.

	Low	Medium	High
Legal	Disruptions of guidelines and rules with slight consequences (slight breaks of agreement which result in at most inconsiderable contractual consequences).	Disruptions of guidelines and rules with considerable consequences (major breaks of agreement with high contractual consequences).	Major disruptions of guidelines and rules (breaks of contract with disastrous damage liabilities).
Organizational	Damage with no or few effects on business purposes, customers, or business partners.	Damage of the ability to carry out the tasks, so one or more business purposes will not succeed and there is a negative impact on customers and business partners.	Damage of the ability to carry out tasks was evaluated as unbearable and one or more major business purposes will not succeed and long term negative effects on customers and business partners.

Table 1. *Cont.*

	Low	Medium	High
Technical	There is no significant infrastructure or technology impacted. No key assets involved.	There is a single significant infrastructure or technology impacted. Single vulnerability of a standard infrastructural asset involved.	There are several significant infrastructures or technologies impacted. There are several vulnerabilities of standard infrastructural assets involved.
Cultural	There is no or little impact on cultural mentality in the organization or the customer base.	There is expected negative effects in 1-2 related aspects of the cultural mentality in the organization or the customer base.	There is an expected negative impact in more than two related aspects of the cultural mentality in the organization or the customer base.
Financial	The financial damage is substantial, but does not intimidate the existence of the organization.	The financial damage is significant, and could intimidate the existence of the organization.	The financial damage intimidates the existence of the organization.

Dependencies exist between various equipment that have influence over the classification to a specific degree. The following rules should be considered for the inheritance:

Maximum rule: By the definition of the maximum rule, the classification of a resource is described as the highest requirement level of a process, which utilizes that resource or in other words, a piece of information that is treated by that resource.

Accumulation: If multiple, less significant resources are dependent on a single resource and the total of these resources or the affection of integrity and the level of availability confidentiality results in a higher harm (higher classification) than the affection of a single resource, then, the accumulation effect occurs.

Distribution: The opposite of the accumulation effect is the distribution effect, which occurs when the area of application of a resource is spread over a number of other resources. Hence, the classification of such a resource can be lowered.

The distribution effect is supposed to be applied over the discrete resources beginning at the application level.

2.2. Validation of the Framework by Experts

To confirm the validity of a framework, there is a need for the opinion of multiple experts of the field. As a result, the possibility of modification, adaption, and improvement of the primary design is provided. Hence, it is necessary to obtain a complete understanding of the subjective comments of experts to select an interpretive theoretical perspective. A person who has the required skills and credentials in his or her profession to operate at the maximum level of quality is known to be an expert [47]. This method automatically results in a qualitative approach, with techniques that include important interactions with people directly experiencing the phenomena under study. The justification by experts designed for this activity was developed using two different steps.

1. Assessment of every element of the framework in an isolated mode to assure that the tools existing in each element of the framework (questionnaires) are valid, as well as examining the validity of the considered questions.

2. Assessment of the framework to ensure the validity as a whole by respected experts of the field.

In the following section, the two processes and their results are presented.

2.2.1. Validation of the Items

The details of the framework elements to be evaluated for validity (legal, technological, processual/organizational, cultural) needs separate groups of professionals in their respective fields. Hence, evaluation was carried out in separate processes that are defined for each field in the following. With respect to the detailed approach adopted to perform the validation, it is according to experts' workshops. The aim of these workshops is the validation of the questionnaire.

The selection of experts was different for each item and was different to present information in a more reduced form. Table 2 includes the selection criteria of the four items:

Table 2. Item validation selection criteria, candidates, and final set of experts.

	Legal	Technological	Processual/Organizational	Cultural
University Education	Master in Law or IT Management	Master in IT Management	Master in Management	Master in Management, Human Resource Management
Professional Knowledge	Business English Legal English	Business English Legal English (Optional)	Business English Legal English (Optional)	Business English Legal English (Optional)
Candidates contacted	15	15	15	15
Candidates selected	4	3	5	3

Moreover, the common requisite for all is the needed experience: Five years in a relevant area and two years in decision making.

The selected experts were provided with a detailed description of the proposed framework in the item assessed. The workshop was facilitated and conducted by at least one researcher on site. Furthermore, they were given some particular questions that they were requested to answer at the workshop:

- Whether the provided framework is an adequate tool to describe risks?
- Whether there are other fields for affections or risks for cloud computing/cloud services?
- If yes, what are these other fields?
- What is the significance of each of the provided fields from the point of view of the experts?
- Are questionnaires sufficient to find inputs in the certain subject area for the goal of risk evaluation of the framework?
- Whether there are any questions that are imprecisely expressed or other explanations are necessary?
- Whether there are any questions that are not essential or unnecessary and hence should be deleted from the questionnaire?
- Are there any related questions that have not been taken into account until now and should therefore be added to the questionnaire?
- Are there any more comments or recommendations.

The result of this validation was a set of changes in the inclusion or exclusion of questions, clarifications of terms, and rewording. Generally, the process of validation gave the planned benefits for the framework. Along with the assessment and enhancement of elements in the various subject fields, it provided an essential and beneficial multi-disciplinary view of the framework. The particular worldviews of the experts in the various fields can be described as follows:

A. There is a need for concise description of the legal fields considered by the experts, e.g., the description of “change”.
B. The professionals from the processual and organizational field focused on the requirement of precise procedure classifications from the organizational point of view (e.g., “governance processes”, “core processes”, “support processes”) and from the point of view of their essentiality (“must-do”, “nice-to-have”, “delighter”). Adding to that, they underlined the significance of KPIs relevant to particular techniques and suggested an extended quantification-oriented method of the questionnaire.
C. The experts from the technological field emphasized the significance of technological developments and advancements and of particular employment and implementation methods.
D. The experts from the cultural field identified additional potential fields of affection (military, politics) and emphasized the significance of particular cultural aspects in certain countries or cultures.

2.2.2. Validation of the Framework as a Whole

In this case, a questionnaire was designed and sent via email to the experts. The main questions included in the artefact are:

A. Correctness in the focus of the framework.
B. Opinion on the methodology adopted.
C. Opinion on the theoretical contribution of the framework.
D. Opinion on the applicability of the framework.
E. Opinion on the artefacts (questionnaires) included.

The questionnaire was delivered to respected professionals by email. Experts completed the questionnaire remotely with the assistance of researchers. The questionnaire includes open questions that asks about different dimensions: Methodological importance, theoretical innovation, practical usability, etc.

Experts were chosen from academia as well as the industry, with the help of some methods. The number of possible interviewees from the industry were recognized according to the previous working connections and other network interacting activities. Possible applicants from academia were recognized based on personal relationships. To contribute to this study, 15 experts in the area were requested by e-mail to contribute and six of them accepted the request. Contributors were fully informed about the implications of their participation in the research, and to fulfil the ethical matters, every expert was given a research profile.

The main results from the assessment of the questionnaires are as follows:

- Framework goals: All chosen professionals have encouragingly evaluated the main objective of the framework. The experts know that because of the generalization of cloud computing and the rising stress on compliance management, research to encourage an awareness and exercise of compliance is essential.
- Methodology: Experts have decided that the design and usage of qualitative methodological methods and literature reviews guarantee the building of a suitable framework.
- Theoretical innovation: Up to now, there is little literature devoted to the improvement of efficiency of the compliance procedure in cloud computing settings. The outcomes acquired from the implementation of the framework will signify an improvement in the knowledge of the management of compliance issues. Accordingly, experts expect that the implementation of the framework will approve the relevance of the procedure and, at the same time, approve the requirement for frameworks to guide the management of these procedures.
- Applicability: It is possible to apply the result of implementing the framework to other projects and there is even the potential to generate the need to develop frameworks in order to guide other main processes in a cloud computing environment.
- Suggestions for improvement: According to the areas for development or manipulation, the following facets should be considered:

    - One expert records the time taken in the questionnaires and the need to consider certain support for the implementation of the framework. He comments that to increase the effect of a potential future commercialization, there is a need for more automated support.
    - Another expert is taking care of the maintainability of various dimensions of the framework. This subject thinks that some of the characteristics of the framework will experience volatility and obsolescence.
    - A number of characteristics of the framework were stated by experts that will lead to the improvement of the questionnaires in terms of language to improve the readability. Therefore, the process led to several phrases that were rewritten based on the experts' opinions.

3. Evaluation

The goal of the evaluation is to confirm that the developed framework enhances compliance management in cloud computing environments. The fundamental impression behind this evaluation is to compare the performance of the institutional change management in a cloud service setting before and after introduction of the proposed framework. This comparison will be performed comparing KPIs pre and post framework adoption.

There is a need that the organization in which the mentioned evaluation is carried out meets specific criteria that were defined previously. The respected organizations should carry a specific maturity of their IT processes so that the subjects of institutional change management, compliance, and cloud services have the appropriate relevancy for the organization. It is preferred that the mentioned organizations are owned by the private sector and are being active in the open market to replicate the main approach of the framework (e.g., not restricted to public authorities only). Adding to that is the assurance of implementing the framework within the organization in such a way that it becomes full and sincere. It is significant that the contact person in the organization has the adequate position to be able to affect and achieve the required IT and risk management decisions and methods that are accompany the framework at the corporate level. In the following are the explanations of the key features of the evaluation plan.

Two organizations agreed to participate in the evaluation. Organization A is an insurance company from Germany offering a full range of insurance services to its clients. Its caveats are as follows:

- Increasing expenses for IT compliance because of the loss of the IT compliance function in the organization; and
- excessive risks linked with non-compliance that cannot be quantified at the moment.

Organization B is an IT service provider that offers a range of IT services to institutional customers only. According to the information provided, B wants to address the following aspects:

- Increased capability in articulating its own IT compliance to present and potential customers; and
- to assure compliance of IT processes for customers with uppermost essentials, e.g., defense and intelligence agencies.

The specific aims for both companies to adopt the framework are as follows:

- To prevent the so called “conformity-gaps” between requirements and their real implementation in IT;
- implementing the changes in holistic, risk-oriented concerns of IT compliance;
- to govern the requirements and a higher level of standardization during the process of implementation (increase in maturity levels);
- to ensure the compliance of IT processes, for example, by closing existing non-compliance outcomes and an established compliance with current regulations; and
- decrease the probability of an occurrence and the possible harm of risks.

A compliance evaluation sheet was designed and sent to both organizations in the pre (I) and post (II) framework adoption phases. In the following, comparisons between I and II in each case study in an isolated way will be conducted, and in the last subsection, a comparison between the case studies and phases will also be presented. There are two sources of information gathered via two sets of information. Firstly, the Compliance Evaluation Sheet and, secondly, the Compliance Metrics Questionnaire. With regards to the first, the general structure is as follows:

- Typical data on participant:
  - Sex;
  - age;
  - position;
  - years of professional experience; and
  - years of experience in the position.
- Management of compliance.
- Level of overall satisfaction with compliance management in CC (Very satisfied; Satisfied; Neither; Dissatisfied; Very dissatisfied).
- Level of overall satisfaction with CC service (Very satisfied; Satisfied; Neither; Dissatisfied; Very dissatisfied).
- Level of overall insight on the influence of compliance management in CC on the quality of service of IT (Very High; Above Average; Average; Below Average; Very Low).
- Level of overall insight on the influence of compliance management in CC to the organizational compliance management procedures (Very High; Above Average; Average; Below Average; Very Low).

Additionally, a document must be filled out by the CIO, Compliance Manager, or a similar role: The Compliance Metrics Questionnaire, including the following information:

- Average time gap between identification of external compliance problems and resolution;
- number of compliance problems in which employees request direction or support;
- number of reports of unproven or actual compliance violations;
- percentage of compliance enhancement opportunities which are implemented; and
- frequency (in days) in reviews of compliance.

3.1. Case Study 1: Organization A

Eleven respondents answered the Compliance Evaluation Sheet. Three roles are represented in the sample: CIO (9.09%), Manager (36.36%), and Group Leader (54.55%). The second questionnaire was answered just by the CIO of the company. With regards to the first questionnaire, descriptive statistics are shown in Table 3.

Table 3. Descriptive statistics on compliance evaluation sheet. Case Study 1.

	Phase I		Phase II	
	M	**SD**	**M**	**SD**
Satisfaction on cloud services	3.91	.539	4.09	.539
Satisfaction on CM in cloud	3.36	.809	4.00	.632
CM contribution to IT quality of service	3.09	.701	3.73	.786
CM contribution to the organizational CM	2.82	.405	3.64	.674

Generally, it is noteworthy that all the mean values are higher in Phase II compared to Phase I, while standard deviations differ. The only case in which it stays stable is in the first variable, while it is lower with the case of satisfaction with the compliance management in cloud computing. Thus, it is concluded that there is less dispersion of the respondents with respect to their opinion being in a higher agreement. Furthermore, the agreement is achieved with a superior satisfaction. Anyhow, there is a higher satisfaction rate, regarding variables three and four, in Phase II than in Phase I.

The second step in the analysis is the comparison of results between the phases. To do so, the Student's t-test was used. The only aspect in which there are statistical differences is in the last one: $t(10) = -3.451$, $p < 0.05$.

Table 4 presents a comparison of the compliance metrics.

Table 4. Compliance metrics, comparison of phases. Case Study 2.

Metric	Phase I	Phase II
Avg. time between identification of external compliance issues and resolution	48	45
# of compliance issues where employees seek guidance/assistance	19	20
# of reports of alleged or actual compliance violations	89	60
% of compliance opportunities implemented	73	79
Yearly compliance reviews	6	6

Main aspects in the compliance metrics are as follows:

1. Considering the average time span between identification of external compliance issues and resolution, Phase 2 illustrates a minor difference (6.25%) in the resolution of compliance issues after implementing the framework. There is a very limited difference, although, it is possible to see it as a good sign in favor of the adoption of the framework.

2. Considering the number of compliance problems in which employees require advice or support, Phase 2 demonstrate an increase (5.26%) in the problem compliance framework for alteration of the management in the cloud setting identified in which employees require assistance. Again, differences are very minor, however, it is valuable to mention that the framework has potential to guide employees towards a process of guiding them to the correct management of issues, including guidance among its steps.

3. Regarding the number of reports of supposed or actual compliance, violations figures reduced from 89 to 60 (32.59%). Although these facts are very inspiring, the authors want to highlight that the sample size was rather small and the generalization of results is endangered by the unlikelihood of isolating the external factors from the variables. Anyhow, it should be considered that the enhancement is aligned with the rest of the metrics provided.

4. Concerning the percentage of compliance enhancement opportunities implemented, it can be seen that there is again a minimum improvement (8.22%). This is also a sign of the validity of the framework for the effectiveness and efficiency of the management of compliance problems.

5. The last part regarding the frequency (in days) of compliance reviews stays stable. In this case, the organization in Phase 1 offered a compliance management procedure, where reviews were considered to be part of the process. This process stays without any changes in Phase II.

3.2. Case Study 2: Organization B

Ten respondents answered the Compliance Evaluation Sheet. Four roles are represented in the sample: CIO (10%), Vice-president (10%), Manager (20%), and Group Leader (60%). The second questionnaire was answered just by the CIO of the company. With regards to the first questionnaire, the descriptive statistics are shown in Table 5.

Table 5. Descriptive statistics on the compliance evaluation sheet. Case Study 2.

	Phase I		Phase II	
	M	SD	M	SD
Satisfaction on cloud services	4.00	.667	4.40	.516
Satisfaction on CM in cloud	3.70	.823	4.20	.632
CM contribution to IT quality of service	3.10	.568	3.80	.632
CM contribution to the organizational CM	3.10	.568	3.60	.516

Overall, it should be noted once again that the means are, in all cases, higher in Phase II than in Phase I, while standard deviations differ. Considering the first variable, it can be seen that it is lower in Phase II. Variable two and variable four are more dispersed too. It can be concluded that there is less

dispersion in respondents' opinions, thus collecting a higher consensus. Furthermore, the agreement is generated with a higher satisfaction. Anyhow, concerning variable three, there is a higher dispersion in Phase II compared to Phase I. The Student's T test shows a statistical difference in the third aspect of CM's contribution to the IT quality of service, t (9) = −2.605, $p < 0.05$.

With regards to compliance metrics questionnaire, Table 6 shows the data collection:

Table 6. Compliance metrics, comparison of phases. Case Study 2.

Metric	Phase I	Phase II
Avg. time between identification of external compliance issues and resolution	36	35
# of compliance issues where employees seek guidance/assistance	12	11
# of reports of alleged or actual compliance violations	76	58
% of compliance opportunities implemented	75	78
Yearly compliance reviews	12	12

The main aspects in the compliance metrics are as follows:

1. Concerning the average time span between identification of external compliance issues and resolution, Phase 2 illustrates a minor difference (2.18%) in the resolution of compliance issues after the implementation of the framework. There is once again a limited difference, although, it can be considered as a good sign in favor of the adoption of the framework.

2. Considering the number of compliance issues where employees require advice or support, Phase 2 demonstrates a decrease (9.10%) in the problem recognized in which employees ask for support. Once again, differences are minimum and oppose the prior justifications. It is because this can be engrained from a more detailed process implemented with the framework

3. Regarding the number of reports of supposed or actual compliance violations, figures reduced from 76 to 58 (23.78%). Although these facts are very inspiring, we want to highlight that the sample size was reasonably small and the generalization of the results is endangered by the unlikelihood of isolating the external factors from the variables. Anyhow, it is should be considered that the enhancement is aligned with the rest of the metrics provided.

4. Concerning the percentage of compliance enhancement opportunities implemented, it can be seen that there is again a minimum improvement (4%). This is also a sign of the validity of the framework for the effectiveness and efficiency of the management of compliance problems.

5. The last part regarding the frequency (in days) of compliance reviews stays stable. In this case again, the organization in Phase 1 offered a compliance management procedure, where reviews were considered to be part of the process. This process stays without any changes in Phase II.

3.3. Inter Case

In this section, the aggregated data and results for the two cases is presented. Firstly, Table 7 presents aggregated data from both case studies:

Table 7. Descriptive statistics on the compliance evaluation sheet. Inter case.

	Phase I		Phase II	
	M	SD	M	SD
Satisfaction on cloud services	3.95	.590	4.24	.539
Satisfaction on CM in cloud	3.52	.814	4.10	.625
CM contribution to IT quality of service	3.10	.625	3.76	.700
CM contribution to the organizational CM	2.95	.498	3.62	.590

Consistent with previous sections, the means are higher in Phase II, with the standard deviation presenting different values in the variables and cases. The next step is the analysis, by means of the Student's t-test of the significance of the variables. In this case, three of the four variables present

significant values, namely the satisfaction on CM in the cloud t (20) = −2.553, $p < 0.05$; CM contribution to IT quality of service t (20) = −3.255, $p < 0.05$, and, finally, CM contribution to the organizational CM t (20) = −3.960, $p < 0.05$. In a nutshell, this significance means that in the case of the three variables, the framework is able to improve KPIs.

With regards to the Compliance Metrics Questionnaire, Table 8 presents the average of the inter case values.

Table 8. Compliance metrics, comparison of phases. Inter case.

Metric	Phase I	Phase II
Avg. time between identification of external compliance issues and resolution	42	40
# of compliance issues where employees seek guidance/assistance	15.5	15.5
# of reports of alleged or actual compliance violations	82	59.5
% of compliance opportunities implemented	74.5	78.5
Yearly compliance reviews	9	9

Although values are comparable, there are several metrics in which Phase II presents better results, while the only metric with important differences is the number of reports of alleged or actual compliance violations. The authors sees this change as a positive consequence of the implementation of the framework.

4. Discussion, Limitations, Conclusions, and Future Works

The Compliance Evaluation Sheets provide the first set of findings. As stated earlier, the average value of the satisfaction and contribution are higher in Phase II after use, indicating that the framework is positive in the dimensions under consideration. This is probably the most significant outcome of the study, considering this was the aim of this work. Anyhow, it should be noted that, according to the variable of satisfaction on compliance management in the cloud, it is possible that the most significant variable in the questionnaire, apart from a better score (reaching 4.10 from the prior value of 3.52), the standard deviation, was also lower (.625 compared to 0.814). This situation can be seen in the satisfaction with the cloud service too, but provided less variations in the standard deviation scores.

The improvement in satisfaction and involvement of the framework is supported by the fact that there were significant differences in three of the four variables analyzed when comparing the pre and post scenarios (satisfaction on compliance management in CC, t (20) = −2.553, $p < 0.05$; contribution of compliance management in CC to IT quality of service, t (20) = −3.255, $p < 0.05$; and contribution of compliance management in CC to the organizational compliance management, t (20) = −3.960, $p < 0.05$).

Anyhow, it should be noted that the employment of the framework did not influence the satisfaction of the cloud service in a noteworthy way. Since the mean was enhanced and the standard deviation was slightly lower, it was not statistically significant according to the Student T test results (t (20) = −1.639, $p > 0.05$).

Regarding the limitations and threats of validity, the construction of the framework was performed using qualitative methods and threats of validity must be analyzed from this viewpoint. Regarding credibility (as opposed to internal validity of quantitative research), the authors underline that the variety of organizations involved in the construction reduce their influence in the results. Moreover, experts present comparable levels of competence. This leads us to the asseveration that the results are credible from the participants' viewpoint to believably rule out different explanations.

With regards to transferability (external validity in quantitative approaches), again the limited number of subjects in the construction of the framework could harm its transferability. However, again, their comparable level of knowledge and experience improves the generalizability of the artefacts. On the other hand, subjects were invited and selected in a non-random way, so generalization is

not guaranteed; however, replication is possible given the relatively common conditions in which it was defined.

Finally, concerning confirmability (statistical conclusion validity in the quantitative arena), the authors assigned an external auditor in the process to increase the extent in which results could be corroborated.

The validation of the framework was conducted by means of two case studies using quantitative approaches. This needs to be analyzed from the perspective of common quantitative threats. With regards to content validity, the instrument was developed considering current scientific literature, but was also assessed by experts to ensure its content validity. Regarding the conclusion validity, although the sample was modest, the authors believe it was significant enough to assess the framework.

Internal validity could be threatened by the fact that subjects may not present similar levels of knowledge or expertise. To ensure internal validity, participants were chosen with the requisite of presenting a comparable level of competence (knowledge and experience).

External validity is about the generalization of findings. Here, the authors assume two different threats: Sample was not taken randomly and, in the second term, the limited size of the sample.

The proposed framework, built upon the current literature, sheds some light on the differentiation of input areas that need to be considered to guarantee compliance in cloud computing settings. Future work can be focused in different areas of research.

Firstly, a customization of the framework for various functional domains can be developed and assessed. In a second term, a mapping study with relevant standards and initiatives on IT governance, including ISO 38500 or COBIT, should be aimed for in the future, naming just some of the most relevant mappings. Third, the implementation of the framework in various settings to compare national and organizational cultures is also a future aim. In the fourth term, the authors want to expand the framework to tackle aspects of quality of service (QoS) and quality of experience (QoE). Both aspects are very relevant aspects nowadays in the literature of the topic, e.g., [48–54]. While it is true that these nascent initiatives are more relevant to mobile networks, it is also true that these aspects are quite applicable also in organizational cloud scenarios. Finally, the authors are aware of the importance of artificial intelligence technologies in the cybersecurity arena [55–60]. Taking this into account, the authors plan the inclusion of assessment factors to these aspects in future developments of the framework.

Author Contributions: Conceptualization, K.B., S.D., R.C.-P. and V.S.; Data curation, K.B. and S.D.; Formal analysis, K.B., S.D. and R.C.-P.; Investigation, K.B. and S.D.; Methodology, K.B. and S.D.; Supervision, R.C.-P. and V.S.; Validation, R.C.-P. and V.S.; Writing—original draft, K.B. and S.D.; Writing—review & editing, R.C.-P. and V.S.

Funding: This research received no external funding.

Acknowledgments: Authors would like to thank subjects for the contributions provided.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lunardi, G.L.; Becker, J.L.; Maçada, A.C.G.; Dolci, P.C. The impact of adopting IT governance on financial performance: An empirical analysis among Brazilian firms. *Int. J. Account. Inf. Syst.* **2014**, *15*, 66–81. [CrossRef]
2. Mohamad, S.; Toomey, M. A survey of information technology governance capability in five jurisdictions using the ISO 38500:2008 framework. *Int. J. Discl. Gov.* **2016**, *13*, 53–74. [CrossRef]
3. Juiz, C.; Toomey, M. To govern IT, or not to govern IT? *Commun. ACM* **2015**, *58*, 58–64. [CrossRef]
4. Weill, P.; Ross, J.W. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*; Harvard Business Press: Boston, MA, USA, 2004; ISBN 978-1-59139-253-8.
5. Xue, Y.; Liang, H.; Boulton, W.R. Information Technology Governance in Information Technology Investment Decision Processes: The Impact of Investment Characteristics, External Environment, and Internal Context. *MIS Q.* **2008**, *32*, 67–96. [CrossRef]
6. Luftman, J. Assessing It/Business Alignment. *Inf. Syst. Manag.* **2003**, *20*, 9–15. [CrossRef]

7. Henderson, J.C.; Venkatraman, H. Strategic alignment: Leveraging information technology for transforming organizations. *IBM Syst. J.* **1993**, *32*, 472–484. [CrossRef]
8. De Haes, S.; Van Grembergen, W.; Debreceny, R.S. COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *J. Inf. Syst.* **2013**, *27*, 307–324. [CrossRef]
9. Banker, R.D.; Hu, N.; Pavlou, P.A.; Luftman, J. CIO Reporting Structure, Strategic Positioning, and Firm Performance. *MIS Q.* **2011**, *35*, 487–504. [CrossRef]
10. Wu, S.P.-J.; Straub, D.W.; Liang, T.-P. How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers. *MIS Q.* **2015**, *39*, 497–518. [CrossRef]
11. Chi, M.; Zhao, J.; George, J.F.; Li, Y.; Zhai, S. The influence of inter-firm IT governance strategies on relational performance: The moderation effect of information technology ambidexterity. *Int. J. Inf. Manag.* **2017**, *37*, 43–53. [CrossRef]
12. Alreemy, Z.; Chang, V.; Walters, R.; Wills, G. Critical success factors (CSFs) for information technology governance (ITG). *Int. J. Inf. Manag.* **2016**, *36*, 907–916. [CrossRef]
13. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Available online: http://www.isaca.org/cobit/ (accessed on 15 March 2017).
14. Joshi, A.; Bollen, L.; Hassink, H.; De Haes, S.; Van Grembergen, W. Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role. *Inf. Manag.* **2018**, *55*, 368–380. [CrossRef]
15. Weill, P.; Ross, J. A matrixed approach to designing IT governance. *MIT Sloan Manag. Rev.* **2005**, *46*, 26–34.
16. CMMI Product Team. *CMMI for Service, Version 1.3, CMMI-SVC v1. 3*; CMU/SEI-2010-TR-034, Technical Report; Software Engineering Institute: Pittsburgh, PA, USA, 2010.
17. Bianchi, I.S.; Sousa, R.D. IT Governance Mechanisms in Higher Education. *Procedia Comput. Sci.* **2016**, *100*, 941–946. [CrossRef]
18. Khouja, M.; Rodriguez, I.B.; Halima, Y.B.; Moalla, S. IT Governance in Higher Education Institutions: A Systematic Literature Review. *Int. J. Hum. Cap. Inf. Technol. Prof. IJHCITP* **2018**, *9*, 52–67. [CrossRef]
19. Coen, M.; Kelly, U. Information management and governance in UK higher education institutions: Bringing IT in from the cold. *Perspect. Policy Pract. High. Educ.* **2007**, *11*, 7–11. [CrossRef]
20. Grembergen, W.V.; Haes, S.D. IT Governance Structures, Processes and Relational Mechanisms: Achieving IT/Business Alignment in a Major Belgian Financial Group. In Proceedings of the 38th Annual Hawaii International Conference on System Sciences (HICSS), Big Island, HI, USA, 6 January 2005; Volume 8, p. 237b.
21. Robb, A.; Parent, M. Understanding IT Governance: A Case of Two Financial Mutuals. *J. Glob. Inf. Manag. JGIM* **2009**, *17*, 59–77. [CrossRef]
22. Pereira, R.; Almeida, R.; da Silva, M.M. IT Governance Patterns in the Portuguese Financial Industry. In Proceedings of the 2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 6–9 January 2014; pp. 4386–4395.
23. Campbell, J.; McDonald, C.; Sethibe, T. Public and private sector IT governance: Identifying contextual differences. *Australas. J. Inf. Syst.* **2010**, *16*, 5–18. [CrossRef]
24. Wilkin, C.L.; Campbell, J.; Moore, S. Creating value through governing IT deployment in a public/private-sector inter-organisational context: A human agency perspective. *Eur. J. Inf. Syst.* **2013**, *22*, 498–511. [CrossRef]
25. Ali, S.; Green, P. IT Governance Mechanisms in Public Sector Organisations: An Australian Context. *J. Glob. Inf. Manag. JGIM* **2007**, *15*, 41–63. [CrossRef]
26. Pang, M.-S. IT governance and business value in the public sector organizations—The role of elected representatives in IT governance and its impact on IT value in U.S. state governments. *Decis. Support Syst.* **2014**, *59*, 274–285. [CrossRef]
27. Andersen, K.V.; Larsen, M.H.; Pedersen, M.K. IT Governance: Reviewing 17 IT Governance Tools and Analysing the Case of Novozymes A/S. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) (HICSS), Kauia, HI, USA, 4–7 January 2006; Volume 8, p. 195c.
28. Dzombeta, S.; Stantchev, V.; Colomo-Palacios, R.; Brandis, K.; Haufe, K. Governance of Cloud Computing Services for the Life Sciences. *IT Prof.* **2014**, *16*, 30–37. [CrossRef]
29. Deschoolmeester, D.; Devos, J.; Van Landeghem, H. Rethinking IT governance for SMEs. *Ind. Manag. Data Syst.* **2012**, *112*, 206–223.

30. Garbarino-Alberti, H. IT Governance and Human Resources Management: A Framework for SMEs. *Int. J. Hum. Cap. Inf. Technol. Prof. IJHCITP* **2013**, *4*, 40–57. [CrossRef]
31. Shiau, W.-L.; Chau, P.Y.K. Understanding behavioral intention to use a cloud computing classroom: A multiple model comparison approach. *Inf. Manag.* **2016**, *53*, 355–365. [CrossRef]
32. Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019. Available online: https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019 (accessed on 29 November 2018).
33. Chang, V.; Ramachandran, M. Towards Achieving Data Security with the Cloud Computing Adoption Framework. *IEEE Trans. Serv. Comput.* **2016**, *9*, 138–151. [CrossRef]
34. Ramachandran, M. Software security requirements management as an emerging cloud computing service. *Int. J. Inf. Manag.* **2016**, *36*, 580–590. [CrossRef]
35. Huygh, T.; De Haes, S.; Joshi, A.; Van Grembergen, W. Answering key global IT management concerns through IT governance and management processes: A COBIT 5 View. In Proceedings of the 51st Hawaii International Conference on System Sciences, Hawaii, HI, USA, 3 January 2018; pp. 5335–5344.
36. Kim, S. IT compliance of industrial information systems: Technology management and industrial engineering perspective. *J. Syst. Softw.* **2007**, *80*, 1590–1593. [CrossRef]
37. Yimam, D.; Fernandez, E.B. A survey of compliance issues in cloud computing. *J. Internet Serv. Appl.* **2016**, *7*, 5. [CrossRef]
38. van de Weerd, I.; Mangula, I.S.; Brinkkemper, S. Adoption of software as a service in Indonesia: Examining the influence of organizational factors. *Inf. Manag.* **2016**, *53*, 915–928. [CrossRef]
39. Papanikolaou, N.; Pearson, S.; Mont, M.C.; Ko, R.K.L. A toolkit for automating compliance in cloud computing services. *Int. J. Cloud Comput.* **2014**, *3*, 45–68. [CrossRef]
40. Hamdaqa, M.; Hamou-Lhadj, A. An approach based on citation analysis to support effective handling of regulatory compliance. *Future Gener. Comput. Syst.* **2011**, *27*, 395–410. [CrossRef]
41. Kure, H.I.; Islam, S.; Razzaque, M.A. An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Appl. Sci.* **2018**, *8*, 898. [CrossRef]
42. Wheeler, B.C. NEBIC: A Dynamic Capabilities Theory for Assessing Net-Enablement. *Inf. Syst. Res.* **2002**, *13*, 125–146. [CrossRef]
43. Davis, F.D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.* **1989**, *13*, 319–340. [CrossRef]
44. Kluckhohn, F.R.; Strodtbeck, F.L. *Variations in Value Orientations*; Row, Peterson: Evanston, IL, USA, 1961; ISBN 978-0-8371-6740-4.
45. Hofstede, G. *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations Across Nations*, 2nd ed.; SAGE Publications, Inc.: Thousand Oaks, CA, USA, 2003; ISBN 978-0-8039-7324-4.
46. Taylor, S.; Lacy, S.; Macfarlane, I. *ITIL Version 3 Service Transition*; The Office of Government Commerce: San Diego, CA, USA, 2011.
47. Shanteau, J. Competence in experts: The role of task characteristics. *Organ. Behav. Hum. Decis. Process.* **1992**, *53*, 252–266. [CrossRef]
48. Aloqaily, M.; Kantarci, B.; Mouftah, H.T. A Generalized Framework for Quality of Experience (QoE)-Based Provisioning in a Vehicular Cloud. In Proceedings of the 2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), Montreal, QC, Canada, 4–7 October 2015; pp. 1–5.
49. Ridhawi, I.A.; Ridhawi, Y.A. QoS-Aware Service Composition in Mobile Cloud Networks. In Proceedings of the 2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom), Vancouver, BC, Canada, 30 November–3 December 2015; pp. 448–453.
50. Baker, T.; Asim, M.; Tawfik, H.; Aldawsari, B.; Buyya, R. An energy-aware service composition algorithm for multiple cloud-based IoT applications. *J. Netw. Comput. Appl.* **2017**, *89*, 96–108. [CrossRef]
51. Aloqaily, M.; Balasubramanian, V.; Zaman, F.; Al Ridhawi, I.; Jararweh, Y. Congestion Mitigation in Densely Crowded Environments for Augmenting QoS in Vehicular Clouds. In Proceedings of the 8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications, Montreal, QC, Canada, 28 October–2 November 2018; pp. 49–56.
52. Baker, T.; Ugljanin, E.; Faci, N.; Sellami, M.; Maamar, Z.; Kajan, E. Everything as a resource: Foundations and illustration through Internet-of-things. *Comput. Ind.* **2018**, *94*, 62–74. [CrossRef]

53. Roque, J.; Chauvel, L.; Aloqaily, M.; Kantarci, B. A Feasibility Study on Sustainability-Driven Infrastructure Management in Cloud Data Centers. In Proceedings of the 2018 IEEE Canadian Conference on Electrical Computer Engineering (CCECE), Quebec City, QC, Canada, 13–16 May 2018; pp. 1–4.
54. Ridhawi, I.A.; Aloqaily, M.; Kotb, Y.; Ridhawi, Y.A.; Jararweh, Y. A collaborative mobile edge computing and user solution for service composition in 5G systems. *Trans. Emerg. Telecommun. Technol.* **2018**, *29*, e3446. [CrossRef]
55. Otoum, S.; Kantarci, B.; Mouftah, H.T. Detection of Known and Unknown Intrusive Sensor Behavior in Critical Applications. *IEEE Sens. Lett.* **2017**, *1*, 1–4. [CrossRef]
56. García-Crespo, Á.; Gómez-Berbís, J.M.; Colomo-Palacios, R.; Alor-Hernández, G. SecurOntology: A semantic web access control framework. *Comput. Stand. Interfaces* **2011**, *33*, 42–49. [CrossRef]
57. Ghafir, I.; Saleem, J.; Hammoudeh, M.; Faour, H.; Prenosil, V.; Jaf, S.; Jabbar, S.; Baker, T. Security threats to critical infrastructure: The human factor. *J. Supercomput.* **2018**, *74*, 4986–5002. [CrossRef]
58. Otoum, S.; Kantarci, B.; Mouftah, H.T. Mitigating False Negative intruder decisions in WSN-based Smart Grid monitoring. In Proceedings of the 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 26–30 June 2017; pp. 153–158.
59. Stantchev, V.; Colomo-Palacios, R.; Niedermayer, M. Cloud Computing Based Systems for Healthcare. *Sci. World J.* **2014**, *2014*, e692619. [CrossRef] [PubMed]
60. Otoum, S.; Kantarci, B.; Mouftah, H. Adaptively Supervised and Intrusion-Aware Data Aggregation for Wireless Sensor Clusters in Critical Infrastructures. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.